Guide de l'utilisateur pour AsyncOS 14.5 pour Cisco Secure Web Appliance– GD (déploiement général)

Première publication : 2022-04-11

Dernière modification : 2022-07-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

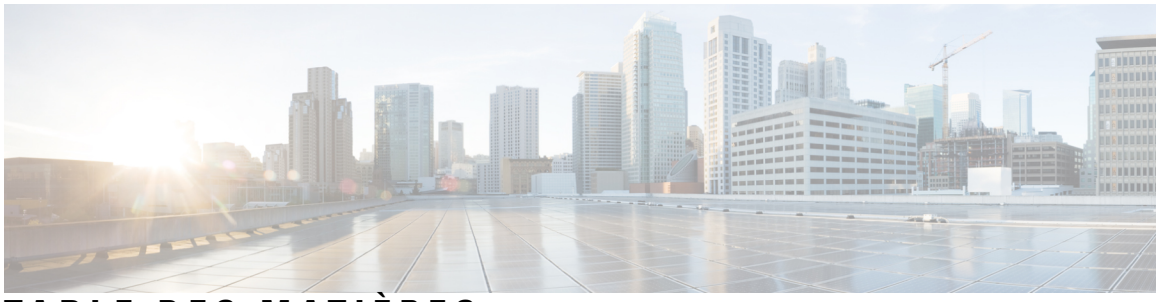
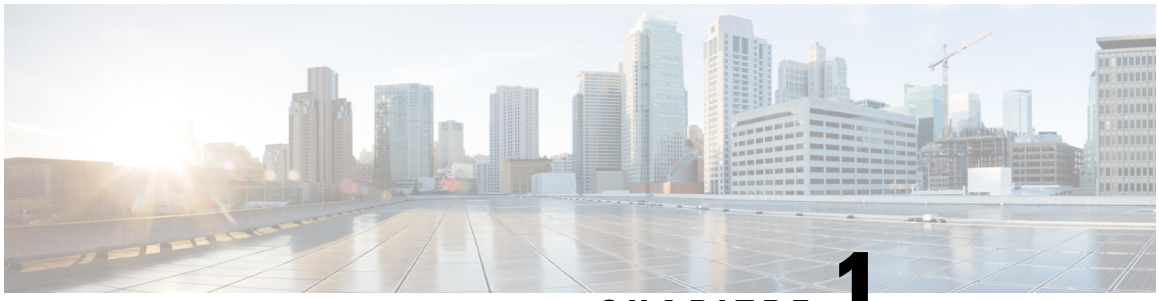


TABLE DES MATIÈRES



CHAPITRE 1

Introduction

Cette rubrique contient les sections suivantes :

À propos de Secure Web Appliance

Cisco Secure Web Appliance (SWA) intercepte et surveille le trafic Internet et applique des politiques pour assurer la protection de votre réseau interne contre les programmes malveillants, la perte de données sensibles, la perte de productivité et d'autres menaces Internet. Secure Web Appliance de Cisco agit comme un serveur proxy, en interceptant les demandes Web des utilisateurs et en analysant le contenu Web demandé à la recherche de menaces potentielles telles que des programmes malveillants, des virus et des tentatives d'hameçonnage. Diverses technologies de sécurité sont utilisées, par exemple le filtrage d'URL, l'analyse antivirus, le filtrage basé sur la réputation et Advanced Malware Protection pour assurer la sécurité du trafic Web. Dans l'ensemble, Secure Web Appliance aide les organisations à sécuriser leur trafic Web, à appliquer les politiques d'utilisation et à se protéger contre les menaces Web, ce qui contribue à créer un environnement de navigation Web plus sûr et plus contrôlé pour les utilisateurs.

Thèmes connexes

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

Utilisation de l'interface Web de l'appliance

Exigences du navigateur de l'interface Web

Voici les exigences pour accéder à l'interface Web :

- Les témoins et JavaScript doivent être pris en charge et activés par votre navigateur.
- Le navigateur doit être en mesure d'afficher des pages HTML contenant des feuilles de style en chaîne (CSS).
- L'Cisco Secure Web Appliance suit les environnements cibles définis par YUI : http://yuilibrary.com/yui/environments/
- Votre session expire automatiquement après 30 minutes d'inactivité.
- Certains boutons et liens de l'interface Web entraînent l'ouverture de fenêtres supplémentaires. Par conséquent, vous devrez peut-être configurer les paramètres de blocage des fenêtres contextuelles du navigateur pour utiliser l'interface Web.

Note N'utilisez qu'une seule fenêtre ou un seul onglet de navigateur à la fois pour modifier la configuration de l'appliance. Ne modifiez pas l'appliance en même temps à l'aide de l'interface Web et de l'interface de ligne de commande. La modification simultanée de l'appliance à partir de plusieurs emplacements entraîne un comportement inattendu et n'est pas prise en charge.

Pour accéder à l'interface graphique, votre navigateur doit prendre en charge JavaScript et être activé pour accepter JavaScript, et il doit être en mesure d'afficher les pages HTML contenant des feuilles de style en chaîne (CSS).

Table 1: Navigateurs et versions pris en charge

Navigateur	Windows 10	MacOS 10.6
Safari	—	version 7.0 ou ultérieure
Google Chrome	Dernière version stable	Dernière version stable
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	Dernière version stable	Dernière version stable
Microsoft Edge	Dernière version stable	Dernière version stable

Les navigateurs ne sont pris en charge que pour les systèmes d'exploitation officiellement pris en charge par le navigateur.

Vous devrez peut-être configurer les paramètres de blocage des fenêtres contextuelles de votre navigateur pour utiliser l'interface graphique, car certains boutons ou certains liens de l'interface entraîneront l'ouverture de fenêtres supplémentaires.

Vous pouvez accéder à l'ancienne interface Web de l'appliance sur n'importe lequel des navigateurs pris en charge.

La résolution prise en charge pour la nouvelle interface Web de l'appliance (AsyncOS 11.8 et versions ultérieures) est comprise entre 1 280 x 800 et 1 680 x 1 050. La meilleure résolution d'affichage pour tous les navigateurs pris en charge est de 1 440 x 900.

Note Cisco ne recommande pas d'afficher la nouvelle interface Web de l'appliance avec des résolutions plus élevées.

Activation de l'accès à l'interface Web sur les appliances virtuelles

Par défaut, les interfaces HTTP et HTTPS ne sont pas activées sur les appliances virtuelles. Pour activer ces protocoles, vous devez utiliser l'interface de ligne de commande.

Étape 1 Accédez à l'interface de commande en ligne. Consultez Accès à l'interface de commande en ligne, on page 667.

Étape 2 Exécutez la commande `interfaceconfig`.

Appuyez sur Enter (Entrée) à une invite pour accepter la valeur par défaut.

Recherchez les invites pour HTTP et HTTPS et activez le ou les protocoles que vous utiliserez.

Recherchez les invites de l'API AsyncOS (supervision) pour HTTP et HTTPS et activez le ou les protocoles que vous utiliserez.

Accès à l'interface Web de l'appliance

Si vous utilisez une appliance virtuelle, consultez Activation de l'accès à l'interface Web sur les appliances virtuelles , on page 3.

Étape 1 Ouvrez un navigateur et entrez l'adresse IP (ou le nom d'hôte) de Secure Web Appliance. Si l'appliance n'a pas été configurée précédemment, utilisez les paramètres par défaut :

`https://192.168.42.42:8443`

-ou-

`http://192.168.42.42:8080`

où `192.168.42.42` est l'adresse IP par défaut, `8080` est le paramètre du port d'administration par défaut pour HTTP et `8443` est le port d'administration par défaut pour `HTTPS`.

Sinon, si l'appliance est actuellement configurée, utilisez l'adresse IP (ou le nom d'hôte) du port M1.

Note Vous devez utiliser un numéro de port lors de la connexion à l'appliance (par défaut, le port `8080`). Le fait de ne pas spécifier de numéro de port lors de l'accès à l'interface Web entraînera l'affichage d'un port par défaut 80, une page d'erreur proxy sans licence.

Étape 2 [Nouvelle interface Web uniquement] Connectez-vous à l'ancienne interface Web et cliquez sur **Secure Web Appliance pour obtenir une nouvelle apparence. Essayez** pour accéder à la nouvelle interface Web! Lorsque vous cliquez sur ce lien, un nouvel onglet s'ouvre dans votre navigateur Web et vous conduit à

`https://wsa_appliance.com:<trailblazer-https-port>/ng-login`, où `wsa_appliance.com` est le nom d'hôte de l'appliance et `<trailblazer-https-port>` est le port HTTPS trailblazer configuré sur l'appliance.

Note

- Vous devez vous connecter à l'ancienne interface Web de l'appliance.
- Assurez-vous que votre serveur DNS peut résoudre le nom d'hôte d'interface de l'appliance que vous avez spécifié.
- Par défaut, la nouvelle interface Web a besoin des ports TCP 6080, 6443 et 4431 pour être opérationnelle. Assurez-vous que ces ports ne sont pas bloqués dans le pare-feu d'entreprise.
- Le port par défaut pour accéder à la nouvelle interface Web est 4431. Cela peut être personnalisé à l'aide de la commande d'interface de ligne de commande `trailerblazerconfig`. Pour plus d'informations sur la commande d'interface de ligne de commande `trailblazerconfig`, consultez Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671.
- La nouvelle interface Web a également besoin de ports d'API AsyncOS (supervision) pour HTTP et HTTPS. Par défaut, ces ports sont 6080 et 6443. Les ports de l'API AsyncOS (supervision) peuvent également être personnalisés dans la commande d'interface de ligne de commande `interfaceconfig`. Pour plus d'informations sur la commande d'interface de ligne de commande `interfaceconfig`, voir Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671.

  Note Les ports sont activés par défaut, mais une fois désactivés, ils seront réactivés après la mise à niveau.

- Si vous modifiez ces ports par défaut, assurez-vous que les ports personnalisés de la nouvelle interface Web ne doivent pas non plus être bloqués dans le pare-feu d'entreprise.

Étape 3 Lorsque l'écran de connexion de l'appliance s'affiche, saisissez votre nom d'utilisateur et votre phrase secrète pour accéder à l'appliance.

Par défaut, l'appliance est livrée avec le nom d'utilisateur et la phrase secrète suivants :

- Nom d'utilisateur : **admin**
- Phrase secrète : **ironport**

Si c'est la première fois que vous vous connectez avec le nom d'utilisateur **admin** par défaut, vous serez invité à modifier immédiatement la phrase secrète.

Étape 4 Pour afficher une liste des tentatives d'accès récentes à l'appliance, réussites ou échecs, pour votre nom d'utilisateur, cliquez sur l'icône d'activité récente (**i** ou **!** en cas de réussite ou d'échec respectivement) devant l'entrée « Logged in as » (Connecté en tant que) dans le coin supérieur droit de la fenêtre de l'application.

Validation des modifications dans l'interface Web

Étape 1 Cliquez sur **Commit Changes** (Valider les modifications).

Étape 2 Entrez des commentaires dans le champ Commentaire si vous le souhaitez.

Étape 3 Cliquez sur **Commit Changes** (Valider les modifications).

Note Vous pouvez apporter plusieurs modifications à la configuration avant de toutes les valider.

Effacement des modifications dans l'interface Web

Étape 1 Cliquez sur **Commit Changes** (Valider les modifications).

Étape 2 Cliquez sur **Abandon Changes** (Ignorer les modifications).

Langues prises en charge

AsyncOS peut afficher son interface graphique et son interface de ligne de commande dans l'une des langues suivantes :

- Allemand
- Anglais
- Espagnol
- Français
- Italien
- Japonais
- Coréen
- Portugais
- Russe
- Chinois
- Taïwanais

Réseau Cisco SensorBase

Le réseau Cisco SensorBase est une base de données de gestion des menaces qui suit des millions de domaines à travers le monde et gère une liste de supervision mondiale du trafic Internet. SensorBase fournit à Cisco une évaluation de la fiabilité des domaines Internet connus. L'Cisco Secure Web Appliance utilise les flux de données SensorBase pour améliorer la précision des scores de réputation Web.

Avantages et confidentialité de SensorBase

La participation au réseau Cisco SensorBase signifie que Cisco recueille des données et les partage avec la base de données de gestion des menaces SensorBase. Ces données comprennent des informations sur les attributs de demande et la façon dont l'appliance traite les demandes.

Cisco reconnaît l'importance du maintien de votre confidentialité et ne recueille ni n'utilise de renseignements personnels ou confidentiels tels que les noms d'utilisateur et les phrases secrètes. En outre, les noms de fichiers et les attributs d'URL qui suivent le nom d'hôte sont masqués pour assurer la confidentialité. En ce qui concerne les transactions HTTPS déchiffrées, le réseau SensorBase reçoit uniquement l'adresse IP, le score de réputation de sites Web et la catégorie d'URL du nom du serveur dans le certificat.

Si vous acceptez de participer au réseau SensorBase, les données envoyées par votre appliance sont transférées de manière sécurisée à l'aide du protocole HTTPS. Le partage des données améliore la capacité de Cisco à réagir aux menaces Web et à protéger l'environnement de votre entreprise contre les activités malveillantes.

Activation de la participation au réseau Cisco SensorBase

Note La participation standard au réseau SensorBase est activée par défaut lors de la configuration du système.

Étape 1 Choisissez **Security Services > SensorBase** (Services de sécurité > SensorBase).

Étape 2 Vérifiez que la participation au réseau SensorBase est activée.

Lorsque cette option est désactivée, aucune donnée collectée par l'appliance n'est renvoyée aux serveurs du réseau SensorBase.

Étape 3 Dans la section du niveau de participation, choisissez l'un des niveaux suivants :

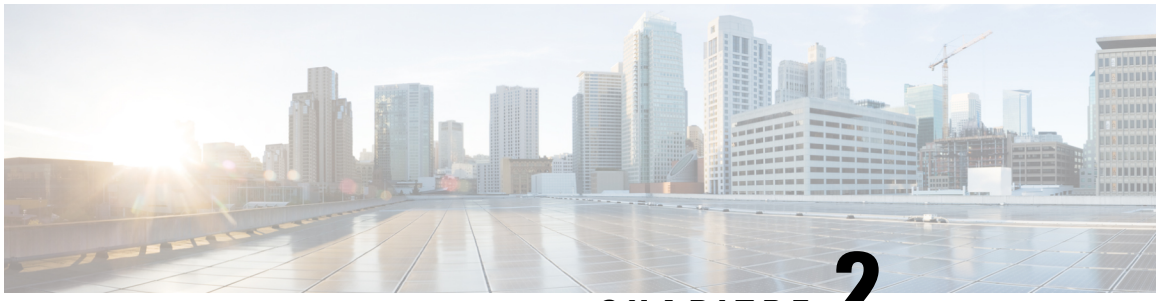
- **Limited** (Limité). La participation de base résume les renseignements sur le nom du serveur et envoie des segments de chemin hachés MD5 aux serveurs du réseau SensorBase.
- **Standard.** La participation améliorée envoie l'URL complète avec des segments de chemin non brouillés aux serveurs du réseau SensorBase. Cette option aide à fournir une base de données plus robuste et améliore continuellement l'intégrité des scores de réputation Web.

Étape 4 Dans le champ AnyConnect Network Participation (Participation au réseau AnyConnect), choisissez d'inclure ou non les informations recueillies auprès des clients qui se connectent aux Cisco Secure Web Appliance à l'aide du client Cisco AnyConnect.

Les clients AnyConnect envoient leur trafic Web vers l'appliance à l'aide de la fonctionnalité Secure Mobility.

Étape 5 Dans le champ Excluded Domains and IP Addresses (Domaines et adresses IP exclus), saisissez facultativement les domaines ou les adresses IP à exclure du trafic envoyé vers les serveurs SensorBase.

Étape 6 Envoyez et validez vos modifications.



CHAPITRE 2

Connexion, installation et configuration

Cette rubrique contient les sections suivantes :

Survol de la connexion, de l'installation et de la configuration

Secure Web Appliance offre les modes de fonctionnement suivants :

- Standard : Le mode standard de fonctionnement Secure Web Appliance comprend les services de proxy Web sur site et la supervision du trafic de la couche 4, qui ne sont pas disponibles dans le mode du connecteur de sécurité Web en nuage.
- Cloud Web Security Connector : en mode Cloud Web Security Connector, l'appliance se connecte et achemine le trafic vers un proxy Cisco Cloud Web Security (CWS), où les politiques de sécurité du Web sont appliquées.

L'appliance dispose de plusieurs ports réseau, chacun affecté pour gérer un ou plusieurs types de données spécifiques.

L'appliance utilise les routages de réseau, le DNS, les VLAN et d'autres paramètres et services pour gérer la connectivité du réseau et l'interception de trafic. L'Assistant de configuration du système vous permet d'installer les services et les paramètres de base, tandis que l'interface Web de l'appliance vous permet de modifier les paramètres et de configurer des options supplémentaires.

Déploiement d'une appliance virtuelle

Pour déployer un Secure Web Appliance virtuel, consultez le *Guide d'installation de l'appliance virtuelle Cisco Content Security Virtual Appliance*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Migration d'une appliance physique vers une appliance virtuelle

Pour migrer votre déploiement d'une appliance physique vers une appliance virtuelle, consultez le guide d'installation de l'appliance virtuelle référencée dans la rubrique précédente et les notes de version de votre version d'AsyncOS.

Comparaison des modes de fonctionnement

Le tableau suivant présente les différentes commandes de menu disponibles dans les modes de connexion Standard et en nuage, en indiquant les diverses fonctionnalités offertes dans chaque mode.

Menu	Disponible en mode standard	Disponible en mode Cloud Connector
Création de rapports	État du système Survol Users (Utilisateurs) Nombre d'utilisateurs Sites Web URL Categories (Catégories d'URL) Visibilité de l'application Protection contre les programmes malveillants Cisco Secure Endpoint Analyse de fichier Mises à jour des verdicts Cisco Secure Endpoint Risques de programmes malveillants des clients Web Reputation Filters (Filtres de réputation Web) Supervision du trafic de la couche 4 Rapports par emplacement d'utilisateur Suivi Web Capacité du système État du système Rapports planifiés Rapports archivés	État du système

Menu	Disponible en mode standard	Disponible en mode Cloud Connector
Responsable de la sécurité Web	Profils d'identification Politiques de routage en nuage Politiques de logiciel-service Politiques de déchiffrement Politiques de routage Politiques d'accès Limites globales de bande passante Sécurité des données Cisco Analyse des programmes malveillants sortants Prévention des pertes de données externes Politiques de dérivation du trafic Web Politiques SOCKS Catégories d'URL personnalisées Définir des plages de temps et des quotas Paramètres de contournement Supervision du trafic de la couche 4	Profils d'identification Politiques de routage en nuage Prévention des pertes de données externes Catégories d'URL personnalisées

Menu	Disponible en mode standard	Disponible en mode Cloud Connector
Services de sécurité	Proxy Web Proxy FTP Proxy HTTPS Proxy SOCKS Hébergement de fichiers PAC Acceptable Use Controls (Contrôles d'utilisation acceptable) Anti-Malware and Reputation (Protection contre les programmes malveillants et réputation) Filtres de transfert de données AnyConnect Secure Mobility Notification à l'utilisateur final L4 Traffic Monitor (Supervision du trafic de la couche 4) SensorBase Création de rapports Cisco Cloudlock Cisco Cognitive Threat Analytics (CTA)	Proxy Web
Réseau	Interfaces Redirection transparente Routs DNS High Availability (Haute disponibilité) Relais SMTP interne Proxy en amont External DLP Servers (Serveurs DLP externes) Dérivation du trafic Web Certificate Management Authentification Fournisseur d'identité pour SaaS Identity Service Engine (ISE)	Interfaces Redirection transparente Routs DNS High Availability (Haute disponibilité) Relais SMTP interne External DLP Servers (Serveurs DLP externes) Certificate Management Authentification Service d'ID d'ordinateur Cloud Connector

Menu	Disponible en mode standard	Disponible en mode Cloud Connector
Administration système	Suivi de politique Alerts (Alertes) Abonnements aux journaux Adresse de retour Configuration SSL Users (Utilisateurs) Accès sécurisé Time Zone (Fuseau horaire) Réglages de l'heure Résumé de la configuration Fichier de configuration Paramètres des clés de fonctionnalité Clés de fonctionnalité Paramètres de mise à niveau et de mise à jour Mise à niveau du système Assistant de configuration du système Mode FIPS Prochaines étapes	Alerts (Alertes) Abonnements aux journaux Configuration SSL Users (Utilisateurs) Accès sécurisé Time Zone (Fuseau horaire) Réglages de l'heure Résumé de la configuration Fichier de configuration Clés de fonctionnalité Paramètres de mise à niveau et de mise à jour Mise à niveau du système Assistant de configuration du système
Portail Cisco CWS (disponible uniquement en mode de sécurité Web hybride)	s.o.	s.o.

Survol des tâches – Connexion, installation et configuration

Tâche	Autres renseignements
Connectez l'appliance au trafic Internet.	Connecter l'appliance, on page 13
Recueillez et enregistrez les informations de configuration.	Collecte d'informations sur la configuration, on page 16
Exécutez l'Assistant de configuration du système.	Assistant de configuration du système, on page 17

Tâche	Autres renseignements
Configurez les paramètres de proxy HTTP, les domaines d'authentification et les profils d'identification. Cette étape doit être effectuée pour le mode de sécurité Web hybride.	Activation du proxy HTTPS, on page 283 Domaines d'authentification, on page 115 Profils d'identification et authentification , on page 162
(Facultatif) Connectez les proxy en amont.	Serveurs proxy en amont, on page 25

Connecter l'appliance

Before you begin

- Pour monter l'appliance, câblez-la pour la gestion et branchez-la au secteur, puis suivez les instructions du guide du matériel de votre appliance. Pour connaître l'emplacement de ce document correspondant pour votre modèle, consultez Documentation, on page 695.
- Si vous prévoyez de connecter physiquement l'appliance à un routeur WCCP v2 pour une redirection transparente, vérifiez d'abord que le routeur WCCP prend en charge la redirection de la couche 2.
- Soyez conscient des recommandations de configuration de Cisco :
  - Utilisez un câblage simplex (câbles distincts pour le trafic entrant et sortant), si possible, pour améliorer les performances et la sécurité.

Étape 1 Connectez-vous à l'interface de gestion si vous ne l'avez pas encore fait :

Ethernet Port (Port Ethernet)	Notes
M1	Connectez M1 à l'emplacement où cela est possible : • Envoyez et recevez du trafic de gestion. • (Facultatif) Envoyez et recevez le trafic de données du proxy Web. Vous pouvez connecter un ordinateur portable directement à M1 pour administrer l'appliance. Pour vous connecter à l'interface de gestion à l'aide d'un nom d'hôte (http://hostname:8080), ajoutez le nom d'hôte et l'adresse IP de l'appliance à la base de données de votre serveur DNS.
P1 et P2 (facultatif)	• Disponible pour le trafic sortant des services de gestion, mais pas pour l'administration. • Activez **Use M1 port for management only** (Utiliser le port M1 pour la gestion uniquement) [page Network > Interfaces (Réseau > Interfaces)]. • Définissez le routage pour que le service utilise l'interface de données.

Étape 2 (Facultatif) Connectez l'appliance au trafic de données directement ou par l'intermédiaire d'un périphérique de redirection transparent :

Ethernet Port (Port Ethernet)	Transfert explicite	Redirection transparente
P1/P2	P1 uniquement : • Activez **Use M1 port for management only** (Utiliser le port M1 pour la gestion uniquement). • Connectez P1 et M1 à des sous-réseaux différents. • Utilisez un câble duplex pour connecter P1 au réseau interne et à Internet pour recevoir le trafic entrant et sortant. P1 et P2 • Activez P1. • Connectez M1, P1 et P2 à différents sous-réseaux. • Connectez P2 à Internet pour recevoir le trafic Internet entrant. Après avoir exécuté l'Assistant de configuration du système, activez P2.	Appareil : routeur WCCP v2 : • Pour la redirection sur la couche 2, connectez physiquement le routeur à P1/P2. • Pour la redirection sur la couche 3, soyez conscient des problèmes de performance possibles avec l'encapsulation de routage générique. • Créez un service WCCP sur l'appliance. Périphérique : Commutateur de couche 4 : • Pour la redirection sur la couche 2, connectez physiquement le commutateur à P1/P2. • Pour la redirection sur la couche 3, soyez conscient des problèmes de performance possibles avec l'encapsulation de routage générique. **Note** L'appliance ne prend pas en charge le mode en ligne.
M1 (facultatif)	Si **Use M1 port for management only** (Utiliser le port M1 pour la gestion uniquement) est désactivé, M1 est le port par défaut pour le trafic de données.	S. O.

Étape 3 (Facultatif) Pour surveiller le trafic de la couche 4, connectez l'appliance à un dérivateur, un commutateur ou un concentrateur après les ports proxy et avant tout périphérique qui effectue la traduction d'adresses réseau (NAT) sur les adresses IP des clients :

Ethernet Port (Port Ethernet)	Notes
T1/T2	Pour autoriser le blocage de la supervision du trafic de la couche 4, placez la supervision du trafic de la couche 4 sur le même réseau que le Secure Web Appliance. **Configuration recommandée :** **Périphérique : Dérivateur réseau :** • **Connectez T1 au dérivateur réseau pour recevoir le trafic client sortant.** • **Connectez T2 au dérivateur réseau pour recevoir le trafic Internet entrant.** Autres options : Périphérique : Dérivateur réseau : • Utilisez un câble duplex sur T1 pour recevoir le trafic entrant et sortant. Périphérique : port réparti ou en miroir sur un commutateur • Connectez T1 pour recevoir le trafic client sortant et connectez T2 pour recevoir le trafic Internet entrant. • (Moins souhaitable) Connectez T1 à l'aide d'un câble semi-duplex ou duplex intégral pour recevoir le trafic entrant et sortant. Périphérique : Concentrateur : • (Le moins souhaitable) Connectez T1 à l'aide d'un câble duplex pour recevoir le trafic entrant et sortant. L'appliance écoute le trafic sur tous les ports TCP de ces interfaces.

Étape 4 Connectez des proxys externes en amont de l'appliance pour permettre aux proxys externes de recevoir les données de l'appliance.

What to do next

Collecte d'informations sur la configuration, on page 16

Thèmes connexes

- Activation ou modification des interfaces réseau, on page 27
- Utilisation de l'interface de données P2 pour les données de proxy Web , on page 42
- Ajout et modification d'un service WCCP, on page 48
- Configuration de la redirection transparente, on page 46
- Serveurs proxy en amont, on page 25

Collecte d'informations sur la configuration

Vous pouvez utiliser la fiche de travail ci-dessous pour enregistrer les valeurs de configuration dont vous aurez besoin lors de l'exécution de l'Assistant de configuration du système. Pour plus d'informations, consultez Informations de référence de l'Assistant de configuration du système, on page 19.

Fiche de travail de l'Assistant de configuration du système			
Propriété	**Valeur**	**Propriété**	**Valeur**
Détails de l'appliance		**Routs**	
Nom d'hôte système par défaut		**Trafic de gestion**	
Serveur(s) DNS local(aux) **(Requis si vous n'utilisez pas de serveurs racine Internet)**		Default Gateway (Passerelle par défaut)	
Serveur DNS 1		(Facultatif) Nom de la table de routage statique	
(Facultatif) Serveur DNS 2		(Facultatif) Réseau de destination avec table de routage statique	
(Facultatif) Serveur DNS 3		(Facultatif) Adresses de routeur de service standard	
(Facultatif) Paramètres de temps		**(Facultatif) Trafic de données**	
Serveur Network Time Protocol		Default Gateway (Passerelle par défaut)	
(Facultatif) Détails du proxy externe		Nom de la table de routage statique	
Nom du groupe de proxys		Table de routage statique, réseau de destination	
Adresse du serveur proxy		**(Facultatif) Paramètres WCCP**	
Numéro de port du proxy		Adresse du routeur WCCP	

Fiche de travail de l'Assistant de configuration du système			
Propriété	**Valeur**	**Propriété**	**Valeur**
Détails de l'interface		Phrase secrète du routeur WCCP	
Port de gestion (M1)		**Paramètres d'administration**	
Adresse IPv4 (obligatoire) Adresse IPv6 (facultatif)		Administrator Passphrase (Phrase secrète de l'administrateur)	
Network Mask (Masque réseau)		Email System Alerts To (Alertes du système par courriel à)	
Hostname (Nom d'hôte)		(Facultatif) Hôte de relais SMTP	
(Facultatif) Port de données (P1)			
IPv4 (facultatif) Adresse IPv6 (facultatif)			
Network Mask (Masque réseau)			
Hostname (Nom d'hôte)			

Assistant de configuration du système

Before you begin

- Connectez l'appliance aux réseaux et aux périphériques. Consultez Connecter l'appliance, on page 13.
- Renseignez la fiche de travail de l'Assistant de configuration du système. Consultez Collecte d'informations sur la configuration, on page 16.
- Si vous configurez une appliance virtuelle :
  - Utilisez la commande `loadlicense` pour charger la licence de l'appliance virtuelle. Pour obtenir des renseignements complets, consultez le *Guide d'installation de Cisco Content Security Virtual Appliance*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.
  - Activez les interfaces HTTP et/ou HTTPS : dans l'interface de ligne de commande (CLI), exécutez la commande `interfaceconfig`.

- Lors de la configuration de l'Assistant de configuration du système, si la licence Smart est activée, les paramètres des services en nuage le seront également, ce qui vous redirigera vers la page des paramètres des services en nuage.
- Notez que les renseignements de référence sur chaque élément de configuration utilisé dans l'Assistant de configuration du système sont disponibles dans Informations de référence de l'Assistant de configuration du système, on page 19.

Warning N'utilisez l'Assistant de configuration du système que lors de la première installation de l'appliance ou si vous souhaitez remplacer complètement la configuration existante.

Étape 1 Ouvrez un navigateur et entrez l'adresse IP de Secure Web Appliance. La première fois que vous exécutez l'Assistant de configuration du système, utilisez l'adresse IP par défaut :

`https://192.168.42.42:8443`

-ou-

`http://192.168.42.42:8080`

où `192.168.42.42` est l'adresse IP par défaut, `8080` est le paramètre du port d'administration par défaut pour HTTP et `8443` est le port d'administration par défaut pour HTTPS.

Sinon, si l'appliance est actuellement configurée, utilisez l'adresse IP du port M1.

Étape 2 Lorsque l'écran de connexion à l'appliance s'affiche, saisissez le nom d'utilisateur et la phrase secrète pour accéder à l'appliance. Par défaut, l'appliance est livrée avec le nom d'utilisateur et la phrase secrète suivants :

- Nom d'utilisateur : `admin`
- Phrase secrète : `ironport`

Étape 3 Vous devez immédiatement modifier la phrase secrète.

Étape 4 Choisissez **System Administration > System Setup Wizard** (Administration système > Assistant de configuration du système).

Si l'appliance est déjà configurée, vous serez averti que vous êtes sur le point de réinitialiser la configuration. Pour continuer avec l'Assistant de configuration du système, cochez la case **Reset Network Settings** (Réinitialiser les paramètres réseau), puis cliquez sur le bouton **Reset Configuration** (Réinitialiser la configuration). L'appliance sera réinitialisée et le navigateur s'actualise pour afficher l'écran d'accueil de l'appliance.

Étape 5 Lisez et acceptez le contrat de licence utilisateur final.

Étape 6 Cliquez sur **Begin Setup** (Commencer l'installation) pour continuer.

Étape 7 Configurez tous les paramètres à l'aide des tableaux de référence fournis dans les sections suivantes, selon les besoins. Consultez Informations de référence de l'Assistant de configuration du système, on page 19.

Étape 8 Examinez les informations de configuration. Si vous devez modifier une option, cliquez sur **Edit** (Modifier) pour cette section.

Étape 9 Cliquez sur **Install This Configuration** (Installer cette configuration).

What to do next

La page *Next Steps* (Étapes suivantes) devrait s'afficher une fois la configuration installée. Cependant, en fonction des paramètres IP, du nom d'hôte ou des paramètres DNS que vous avez configurés lors de l'installation, vous risquez de perdre la connexion à l'appliance à ce stade. Si une erreur « page not found » (page introuvable) s'affiche dans votre navigateur, modifiez l'URL pour refléter les nouveaux paramètres d'adresse et rechargez la page. Continuez ensuite avec les tâches post-installation que vous souhaitez effectuer.

Informations de référence de l'Assistant de configuration du système

Réseau/Paramètres système

Propriété	Description
Default System Hostname (Nom d'hôte du système par défaut)	Le nom d'hôte du système est le nom d'hôte complet utilisé pour identifier l'appliance dans les domaines suivants : • interface de ligne de commande (CLI) • alertes du système • pages de notification et d'accusé de réception de l'utilisateur final • lors de la formation du nom NetBIOS de l'ordinateur lorsque Secure Web Appliance rejoint un domaine Active Directory Le nom d'hôte du système ne correspond pas directement aux noms d'hôte d'interface et n'est pas utilisé par les clients pour se connecter à l'appliance.
DNS Server(s) [Serveur(s) DNS]	• **Use the Internet's Root DNS Servers** (Utiliser les serveurs DNS racine d'Internet) : vous pouvez choisir d'utiliser les serveurs DNS racine d'Internet pour les recherches de service de nom de domaine lorsque l'appliance n'a pas accès aux serveurs DNS de votre réseau. **Note** Les serveurs DNS racine Internet ne résolvent pas les noms d'hôte locaux. Si vous avez besoin de l'appliance pour résoudre les noms d'hôte locaux, vous devez utiliser un serveur DNS local ou ajouter les entrées statiques appropriées au DNS local à l'aide de l'interface de ligne de commande. • **Use these DNS Servers** (Utiliser ces serveurs DNS) : indiquez les adresses du ou des serveurs DNS locaux que l'appliance peut utiliser pour résoudre les noms d'hôte. Voir DNS Settings (paramètres DNS), on page 57 pour plus d'informations sur ces paramètres.

Propriété	Description
NTP Server (Serveur NTP)	Serveur NTP (Network Time Protocol) utilisé pour synchroniser l'horloge système avec d'autres serveurs sur le réseau ou Internet. La valeur par défaut est time.sco.cisco.com.
Time Zone (Fuseau horaire)	Indiquez des renseignements sur le fuseau horaire correspondant à l'emplacement de l'appliance; affecte les horodatages dans les en-têtes des messages et les fichiers journaux.
Mode de fonctionnement de l'appliance	• **Standard** : utilisé pour l'application standard des politiques sur site. • **Cloud Web Security Connector** (connecteur de sécurité Web en nuage) : utilisé principalement pour diriger le trafic vers le service Cloud Web Security de Cisco pour l'application des politiques et la défense contre les menaces. • **Hybrid Web Security**(Sécurité du Web hybride) : utilisée conjointement avec le service Cloud Web Security de Cisco pour l'application des politiques dans le nuage et sur site et pour la défense contre les menaces. Voir Comparaison des modes de fonctionnement, on page 8 pour plus d'informations sur ces modes de fonctionnement.

Réseau/Contexte du réseau

Note Lorsque vous utilisez Secure Web Appliance dans un réseau qui contient un autre serveur proxy, il est recommandé de placer Secure Web Appliance en aval du serveur proxy, plus près des clients.

Propriété	Description
Is there another web proxy on your network? (Existe-t-il un autre proxy Web sur votre réseau?)	Existe-t-il un autre proxy sur votre réseau que le trafic doit traverser? Se trouvera-t-il en amont de Secure Web Appliance? Si la réponse aux deux questions est oui, cochez la case . Cela vous permet de créer un groupe de proxys pour un proxy en amont. Vous pourrez ajouter d'autres proxys en amont plus tard.
Proxy group name (Nom du groupe de proxys)	Nom utilisé pour identifier le groupe de proxys sur l'appliance.
Address (Adresse)	Nom d'hôte ou adresse IP du serveur proxy en amont.
Port	Numéro de port du serveur proxy en amont.

Thèmes connexes

- Serveurs proxy en amont, on page 25

Réseau/Paramètres de Cloud Connector

Besoin de confirmer le nom et les paramètres de la page.

Paramètres	Description
Cloud Web Security Proxy Servers (Serveurs proxy Cloud Web Security)	Adresse du serveur proxy dans le nuage (CPS), par exemple, proxy1743.scansafe.net.
Failure Handling (Gestion des échecs)	Si AsyncOS ne parvient pas à se connecter à un proxy Cloud Web Security, **connectez-vous directement** à Internet ou **abandonnez les demandes**.
Cloud Web Security Authorization Scheme (Schéma d'autorisation Cloud Web Security)	Méthode d'autorisation des transactions : • Adresse IPv4 publique Secure Web Appliance. • Clé d'autorisation incluse avec chaque transaction. Vous pouvez générer une clé d'autorisation dans le portail Cisco Cloud Web Security.

Réseau/Interfaces réseau et câblage

L'adresse IP, le masque de réseau et le nom d'hôte à utiliser pour gérer le trafic Secure Web Appliance et, par défaut, le trafic proxy (de données).

Vous pouvez utiliser le nom d'hôte indiqué ici lors de la connexion à l'interface de gestion de l'appliance (ou dans les paramètres de proxy du navigateur si M1 est utilisé pour les données de proxy), mais vous devez l'enregistrer dans le DNS de votre entreprise.

Paramètres	Description
Ethernet Port (Port Ethernet)	(Facultatif) Cochez la case **Use M1 port for management only** (Utiliser le port M1 pour la gestion uniquement) si vous souhaitez utiliser un port distinct pour le trafic de données. Si vous configurez l'interface M1 pour le trafic de gestion uniquement, vous devez configurer l'interface P1 pour le trafic de données. Vous devez également définir différentes voies de routage pour la gestion et le trafic de données. Cependant, vous pouvez configurer l'interface P1 même lorsque l'interface M1 est utilisée à la fois pour la gestion et le trafic de données. Vous pouvez activer et configurer le port P1 uniquement dans l'Assistant de configuration du système. Si vous souhaitez activer l'interface P2, vous devez le faire après avoir terminé l'Assistant de configuration du système.
IP Address / Netmask (Adresse IP/Masque réseau)	Adresse IP et masque réseau à utiliser lors de la gestion de Secure Web Appliance sur cette interface réseau.
Hostname (Nom d'hôte)	Nom d'hôte à utiliser lors de la gestion de Secure Web Appliance sur cette interface réseau.

Réseau/Câblage de la supervision du trafic de la couche 4

Propriété	Description
Supervision du trafic de la couche 4	Le type de connexions filaires branchées sur les interfaces en « T » : • **Dérivation en duplex.** Le port T1 reçoit le trafic entrant et sortant. • **Dérivation simple.** Le port T1 reçoit le trafic sortant (des clients vers Internet) et le port T2 reçoit le trafic entrant (d'Internet vers les clients). Cisco recommande d'utiliser l'option simplex lorsque cela est possible, car elle peut augmenter les performances et la sécurité.

Réseau/Voies de routage pour la gestion et le trafic de données

Note Si vous activez « Use M1 port for management only » (Utiliser le port M1 pour la gestion uniquement), cette section comprendra des sections distinctes pour la gestion et le trafic des données; sinon, une seule section de jonction sera affichée.

Propriété	Description
Default Gateway (Passerelle par défaut)	Adresse IP de la passerelle par défaut à utiliser pour le trafic dans les interfaces de gestion et de données.
Static Routes Table (Tableau des voies de routage statiques)	Voies de routages statiques facultatives pour la gestion et le trafic des données. Plusieurs voies de routage peuvent être ajoutées. • **Name** (Nom) : nom utilisé pour identifier la voie de routage statique. • **Internal Network** (Réseau interne) : adresse IPv4 pour la destination de cette voie de routage sur le réseau. • **Internal Gateway** (Passerelle interne) : adresse IPv4 de la passerelle pour cette voie de routage. Une passerelle de routage doit résider sur le même sous-réseau que l'interface de gestion ou de données sur laquelle elle est configurée.

Réseau/Paramètres de connexion transparente

Note Par défaut, Cloud Connector est déployé en mode transparent, ce qui nécessite une connexion à un commutateur de couche 4 ou à un routeur WCCP version 2.

Propriété	Description
Layer-4 Switch or No Device (Commutateur de couche 4 ou aucun périphérique)	Indique que Secure Web Appliance est connecté à un commutateur de couche 4 pour une redirection transparente, ou qu'aucun périphérique de redirection transparent n'est utilisé et les clients transféreront explicitement les demandes à l'appliance.

Propriété	Description
WCCP v2 Router (Routeur WCCP v2)	Indique que Secure Web Appliance est connecté à un routeur compatible avec WCCP version 2. Si vous connectez l'appliance à un routeur WCCP version 2, vous devez créer au moins un service WCCP. Vous pouvez activer le service standard à partir de cet écran ou, une fois l'Assistant de configuration du système terminé, où vous pouvez également créer plusieurs services dynamiques. Lorsque vous activez le service standard, vous pouvez également activer la sécurité du routeur et saisir une phrase secrète. La phrase secrète utilisée ici doit être utilisée pour toutes les appliances et routeurs WCCP du même groupe de services. Un type de service standard (également appelé service « web-cache ») se voit attribuer un ID fixe égal à zéro, une méthode de redirection fixe (par port de destination) et un port de destination fixe égal à 80. Un type de service dynamique vous permet de définir un ID personnalisé, des numéros de port et des options de redirection et d'équilibrage de la charge.

Réseau/Paramètres administratifs

Propriété	Description
Administrator Passphrase (Phrase secrète de l'administrateur)	Phrase secrète utilisée pour accéder à Secure Web Appliance à des fins d'administration.
Email System Alerts To (Alertes du système par courriel à)	Adresse de messagerie à laquelle l'appliance envoie des alertes système.
Send Email via SMTP Relay Host (optional) (Envoyer un courriel par l'entremise de l'hôte de relais SMTP [facultatif])	L'adresse et le port d'un hôte de relais SMTP qu'AsyncOS peut utiliser pour envoyer les courriels générés par le système. Si aucun hôte de relais SMTP n'est défini, AsyncOS utilise les serveurs de messagerie répertoriés dans l'enregistrement MX.
AutoSupport (AutoAssistance)	Indique si l'appliance envoie des alertes du système et des rapports d'état hebdomadaires à l'assistance client de Cisco.
SensorBase Network Participation (Participation au réseau SensorBase)	Indique la participation ou non au réseau Cisco SensorBase. Si vous participez, vous pouvez configurer une participation limitée ou standard (complète). L'option Standard est sélectionnée par défaut. Le réseau SensorBase est une base de données de gestion des menaces qui suit des millions de domaines à travers le monde et maintient une liste de supervision mondiale pour le trafic Internet. Lorsque vous activez la participation au réseau SensorBase, Secure Web Appliance envoie des statistiques anonymes de demandes HTTP à Cisco pour augmenter la valeur des données du réseau SensorBase.

Sécurité/Paramètres de sécurité

Option	Description
Global Policy Default Action (Action par défaut de la politique globale)	Indique s'il faut bloquer ou surveiller tout le trafic Web par défaut une fois l'Assistant de configuration du système terminé. Vous pourrez modifier ce comportement ultérieurement en modifiant les paramètres de protocoles et d'agents utilisateurs pour la politique d'accès globale. Le paramètre par défaut consiste en la supervision du trafic.
L4 Traffic Monitor (Supervision du trafic de la couche 4)	Indique si la supervision du trafic de la couche 4 doit surveiller ou bloquer les programmes malveillants suspects par défaut une fois l'Assistant de configuration du système terminé. Vous pourrez modifier ce comportement ultérieurement. Le paramètre par défaut consiste en la supervision du trafic.
Acceptable Use Controls (Contrôles d'utilisation acceptable)	Indique s'il faut activer les contrôles d'utilisation acceptable. S'ils sont activés, les contrôles d'utilisation acceptable vous permettent de configurer des politiques en fonction du filtrage d'URL. Ils offrent également une visibilité et un contrôle des applications, ainsi que des options connexes telles que l'application de la recherche sécurisée. La valeur par défaut est Enabled (Activé).
Reputation Filtering (Filtrage par réputation)	Indique s'il faut activer le filtrage de réputation Web pour le groupe de politiques global. Les filtres de réputation Web sont une fonctionnalité de sécurité qui analyse le comportement d'un serveur Web et attribue un score de réputation à une URL pour déterminer la probabilité qu'elle contienne des programmes malveillants basés sur les URL. La valeur par défaut est Enabled (Activé).
Malware and Spyware Scanning (Analyse des programmes malveillants et des logiciels espions)	Indique s'il faut activer la recherche de programmes malveillants et de logiciels espions à l'aide de Webroot, McAfee ou Sophos. Par défaut, les trois options sont activées. La plupart des services de sécurité sont automatiquement activés ou désactivés pour correspondre aux services normalement disponibles pour les politiques Cisco Cloud. De même, les valeurs par défaut liées aux politiques ne seront pas applicables. Au moins une option d'analyse doit être activée. Si une option est activée, vous pouvez également choisir de surveiller ou de bloquer les programmes malveillants détectés. Le paramètre par défaut est de surveiller les programmes malveillants. Vous pouvez approfondir la configuration de l'analyse des programmes malveillants après avoir terminé l'Assistant de configuration du système.
Cisco Data Security Filtering (Filtrage de sécurité des données Cisco)	Indique s'il faut activer ou non les filtres de sécurité des données Cisco. S'ils sont activés, les filtres de sécurité des données Cisco évaluent les données qui quittent le réseau et vous permettent de créer des politiques de sécurité des données Cisco pour bloquer des types particuliers de demandes de chargement. La valeur par défaut est Enabled (Activé).

Serveurs proxy en amont

Le proxy Web peut transférer le trafic Web directement vers son serveur Web de destination ou utiliser des politiques de routage pour le rediriger vers un proxy externe en amont.

Survol des tâches des serveurs proxy en amont

Tâche	Autres renseignements
• Connectez le proxy externe en amont de Cisco Secure Web Appliance.	Connecter l'appliance, on page 13.
• Créez et configurez un groupe de proxy pour le proxy en amont.	Création de groupes de serveurs proxy pour les serveurs proxy en amont, on page 25.
• Créez une politique de routage pour le groupe de proxy afin de gérer le trafic à acheminer vers le proxy en amont.	Créer des politiques pour contrôler les demandes Internet, on page 247

Création de groupes de serveurs proxy pour les serveurs proxy en amont

Étape 1 Choisissez **Network > Upstream Proxies** (Réseau > Proxys en amont).

Étape 2 Cliquez sur **Add Group** (Ajouter un groupe).

Étape 3 Complétez les paramètres du groupe de proxy.

Propriété	Description
Name (Nom)	Le nom utilisé pour identifier les groupes de proxy sur l'appliance, dans les politiques de routage, par exemple.
Serveurs proxy	L'adresse, le port et les tentatives de reconnexion (dans le cas où un proxy ne répond pas) pour les serveurs proxy du groupe. Des lignes pour chaque serveur proxy peuvent être ajoutées ou supprimées au besoin. **Note** Vous pouvez saisir le même serveur proxy plusieurs fois pour permettre une répartition inégale de la charge entre les proxy du groupe proxy.

Propriété	Description
Équilibrage de la charge	Politique utilisée par le proxy Web pour équilibrer la charge des demandes entre plusieurs proxys en amont. Choisissez parmi : • **None (failover)** (Aucun [basculement]). Le proxy Web dirige les transactions vers un proxy externe du groupe. Il essaie de se connecter aux proxy dans l'ordre dans lequel ils sont répertoriés. Si un proxy ne peut pas être atteint, le proxy Web tente de se connecter au suivant dans la liste. • **Fewest connections** (Le moins de connexions). Le proxy Web assure le suivi du nombre de demandes actives provenant des différents proxys du groupe et dirige une transaction vers le proxy qui traite actuellement le plus petit nombre de connexions. • **Hash based** (Basé sur le hachage). **Least recently used** (Utilisé le moins récemment). Le proxy Web dirige une transaction vers le proxy qui a reçu une transaction le moins récemment si tous les proxys sont actifs. Ce paramètre est similaire au tourniquet, sauf que le proxy Web prend également en compte les transactions qu'un proxy a reçues en étant membre d'un autre groupe de proxy. C'est-à-dire que si un proxy est répertorié dans plusieurs groupes de proxy, l'option « utilisés récemment » est moins susceptible de surcharger ce proxy. • **Round robin** (Circuit cyclique). Le proxy Web distribue les transactions de manière égale entre tous les proxys du groupe dans l'ordre indiqué. **Note** L'option d'équilibrage de la charge est grisée jusqu'à ce que deux proxy ou plus aient été définis.
Failure Handling (Gestion des échecs)	Spécifie l'action par défaut à entreprendre si tous les proxy de ce groupe échouent. Choisissez parmi : • **Connect directly** (Connectez-vous directement). Envoyez les requêtes directement à leurs serveurs de destination. • **Drop requests** (Abandon des demandes). Supprimez les demandes sans les transférer.

Étape 4 Envoyez et validez vos modifications.

What to do next

- Création d'une politique , on page 253

Interfaces réseau

Versions d'adresses IP

En mode standard, Cisco Secure Web Appliance prend en charge les adresses IPv4 et IPv6 dans la plupart des cas.

Note En mode Cloud Connector, Cisco Secure Web Appliance prend en charge IPv4 uniquement.

Un serveur DNS peut renvoyer un résultat avec des adresses IPv4 et IPv6. Les paramètres DNS comprennent une préférence de version d'adresse IP pour configurer le comportement d'AsyncOS dans ces cas.

Interface ou service	IPv4	IPv6	Notes
Interface M1	Requis	Facultatif	L'utilisation d'adresses IPv6 nécessite un tableau de routage IPv6 qui définit la passerelle IPv6 par défaut. Selon le réseau, vous devrez peut-être également spécifier une voie de routage IPv6 statique dans la table de routage.
Interface P1	Facultatif	Facultatif	Si l'interface P1 a une adresse IPv6 configurée et que l'appliance utilise le routage fractionné (gestion et voies de routage de données séparées), l'interface P1 ne peut pas utiliser la passerelle IPv6 configurée sur la voie de routage de gestion. Indiquez plutôt une passerelle IPv6 pour le tableau de routage de données.
Interface P2	Facultatif	Facultatif	—
Services de données	Pris en charge	Pris en charge	—
Services de contrôle et de gestion	Prise en charge	Prise en charge partielle	Les images, par exemple les logos personnalisés sur les pages de notification à l'utilisateur final, nécessitent un protocole IPv4.
AnyConnect Secure Mobility (MUS)	Prise en charge	Aucune prise en charge	—

Thèmes connexes

- Activation ou modification des interfaces réseau, on page 27
- DNS Settings (paramètres DNS), on page 57

Activation ou modification des interfaces réseau

- Ajouter ou modifier des adresses IP d'interface
- Modifier le type de câblage de la supervision du trafic de la couche 4
- Activer le routage fractionné de la gestion et du trafic de données

Étape 1 Choisissez **Network > Interfaces** (Réseau > Interfaces).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Configurez les options de l'interface.

Option	Description
Interfaces	Modifiez ou ajoutez de nouveaux détails sur l'adresse IPv4 ou IPv6, le masque réseau et le nom d'hôte pour les interfaces M1, P1 ou P2, selon les besoins. • **M1** : AsyncOS nécessite une adresse IPv4 pour le port M1 (gestion). Outre l'adresse IPv4, vous pouvez spécifier une adresse IPv6. Par défaut, l'interface de gestion est utilisée pour administrer l'appliance et la supervision du proxy Web (données). Cependant, vous pouvez configurer le port M1 aux fins de gestion uniquement. • **P1** et **P2** : utilisez une adresse IPv4, une adresse IPv6 ou les deux pour les ports de données. Les interfaces de données sont utilisées pour la supervision du proxy Web et le blocage de la supervision du trafic de la couche 4 (facultatif). Vous pouvez également configurer ces interfaces pour prendre en charge les services sortants tels que le DNS, les mises à niveau logicielles, NTP et le trafic de données Traceroute. **Note** Si les interfaces de gestion et de données sont toutes configurées, des adresses IP sur des sous-réseaux différents doivent être attribuées à chacune. **Note** Lorsque le routage fractionné est activé, l'interface de gestion ne peut pas communiquer avec le portail de licences Smart. Pour enregistrer Secure Web Appliance auprès du portail de licences Smart, sélectionnez une interface de données. **Note** Lorsque le routage fractionné est configuré, Secure Web Appliance utilise l'interface de données pour contacter le serveur DLP externe et l'interface de gestion est limitée au trafic de gestion. Ainsi, l'ensemble du trafic DLP est considéré comme du trafic de données plutôt que comme du trafic de gestion lors de l'acheminement du trafic vers le serveur DLP. Par exemple, lorsqu'il y a deux captures de paquets avec les interfaces P1 et M1 filtrées par adresses DLP, le trafic DLP se trouve sur les deux interfaces. Cela est dû au fait que l'interface de gestion envoie des paquets keepalive aux serveurs DLP et le trafic DLP provient des interfaces de données.
Routage distinct des services de gestion	Cochez l'option **Restrict M1 port to appliance management services only** (Restreindre le port M1 aux services de gestion de l'appliance uniquement) pour limiter M1 au trafic de gestion uniquement, ce qui nécessite l'utilisation d'un port distinct pour le trafic de données. **Note** Lorsque vous utilisez M1 pour le trafic de gestion uniquement, configurez au moins une interface de données sur un autre sous-réseau pour le trafic de proxy. Définissez différentes voies de routage pour la gestion et le trafic de données.

Option	Description
Services de gestion d'appliances	Activez ou désactivez l'utilisation des protocoles réseau suivants et spécifiez un numéro de port par défaut : • **FTP** – Désactivé par défaut. • **SSH** • **HTTP** • **HTTPS** En outre, vous pouvez activer/désactiver la redirection du trafic HTTP vers HTTPS.

Étape 4 Envoyez et validez vos modifications.

What to do next

Si vous avez ajouté une adresse IPv6, ajoutez une table de routage IPv6.

Thèmes connexes

- Connecter l'appliance, on page 13.
- Versions d'adresses IP, on page 26
- Configuration des routages de trafic TCP/IP, on page 43

Configuration des cartes d'interface réseau

Cette rubrique contient les sections suivantes :

Paramètres de médias sur les interfaces Ethernet

Vous pouvez accéder aux paramètres de médias pour les interfaces Ethernet à l'aide de la commande **etherconfig**. Chaque interface Ethernet est répertoriée avec ses paramètres actuels. En sélectionnant l'interface, les paramètres de médias applicables sont affichés.

Utilisation de la commande etherconfig pour modifier les paramètres de médias sur les interfaces Ethernet

Utilisez la commande **etherconfig** pour définir les paramètres de duplex (complet/partiel) et la vitesse (10/100/1000 Mbit/s) des interfaces Ethernet. Par défaut, les interfaces sélectionnent automatiquement les paramètres de médias; que vous pouvez remplacer.

Remarque Si vous avez exécuté l'Assistant de configuration du système de l'interface graphique (ou la commande **systemsetup** de l'interface de ligne de commande) comme décrit dans la rubrique Connexion, installation et configuration que vous avez validé les modifications, les paramètres de l'interface Ethernet par défaut devraient déjà être configurés sur votre appliance.

Exemple de modification des paramètres de médias

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
[]> MEDIA
Ethernet interfaces:
1. Management (Autoselect: <1000baseT full-duplex>) 00:50:56:87:a6:46
2. P1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
3. P2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:6a:42
4. T1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
5. T2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:fc:01

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
```

Appairage/association de cartes d'interface réseau

L'appairage de NIC vous permet de combiner deux ports de données physiques pour fournir une interface Ethernet de secours si le chemin de données de la NIC au port Ethernet en amont échoue. Fondamentalement, l'appairage configure les interfaces Ethernet de sorte qu'il y ait une interface principale et une interface de secours. Si l'interface principale tombe en panne (par exemple, si la porteuse entre la carte réseau et le nœud en amont est interrompue), l'interface de secours devient active et une alerte est envoyée. Lorsque l'interface principale est disponible, cette interface devient automatiquement active. Dans la documentation de ce produit, l'appairage de cartes réseau est associé à l'association de cartes réseau.

Note L'appairage de NIC n'est pas disponible sur les passerelles Web S170, S190 et S195.

Vous pouvez créer plusieurs paires de cartes réseau, à condition que vous ayez suffisamment de ports de données. Lors de la création de paires, vous pouvez combiner deux ports de données. Par exemple :

- Data 1 et Data 2
- Data 3 et Data 4
- Data 2 et Data 3

Certaines passerelles Web contiennent une option d'interface réseau à fibre optique. Si elles sont disponibles, vous verrez deux interfaces Ethernet supplémentaires (Data 3 et Data 4) dans la liste des interfaces disponibles sur ces passerelles Web. Dans une configuration hétérogène, ces interfaces gigabit à fibre optique peuvent être jumelées avec les interfaces en cuivre (Data 1, Data 2 et gestion).

Secure Web Appliance ne prend pas en charge la capture de paquets pour les interfaces NIC appairées. La capture de paquets sera appliquée uniquement pour l'interface active. Par exemple, si P1 et P2 sont appairées, P1 et P2 ne seront pas configurées dans l'interface utilisateur ou l'interface de ligne de commande.

Appairage de cartes réseau et VLAN

Les VLAN (voir Augmentation de la capacité de l'interface à l'aide de VLAN) sont autorisés uniquement sur l'interface principale.

Dénomination des paires de NIC

Lors de la création de paires de cartes réseau, vous devez indiquer le nom de la paire. Les paires de cartes réseau créées dans AsyncOS antérieurement à la version 4.5 recevront automatiquement le nom par défaut de « paire 1 » à la suite d'une mise à niveau.

Toute alerte générée sur l'appairage de NIC fera référence à la paire de NIC par son nom.

Appairage de cartes réseau et dispositifs d'écoute existants

Si vous activez l'appairage de cartes réseau sur une interface à laquelle des processus d'écoute sont affectés, vous êtes invité à supprimer, à réaffecter ou à désactiver tous les processus d'écoute affectés à l'interface de secours.

Activation de l'appairage de cartes réseau à l'aide de la commande etherconfig

Note L'appairage de NIC n'est pas disponible sur les passerelles Web S170, S190 et S195.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
Choose the operation you want to perform:
- NEW - Create a new pairing.
[]> NEW
Please enter a name for this pair (Ex: "Pair 1"):
[]> DP1

1. P1
2. P2
Enter the name or number of the primary ethernet interface you wish bind to.
[]> 1

1. P2
2. T1
3. T2
Enter the name or number of the backup ethernet interface you wish to pair.
[]> 2

Paired interfaces:
1. DP1:
        Primary (P1)
        Backup (T1)
```

```
Choose the operation you want to perform:
- NEW - Create a new pairing.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:40:34 2020 MST
example.com> interfaceconfig


Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]> NEW
Ethernet interface:
1. Management
2. DP1
3. P2
[1]> 2
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 192.168.1.2 ):
[]> 10.10.102.66
Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 27
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Hostname:
[]> example.com
Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
2. P1 (10.10.102.66/27 on DP1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]>
example.com>example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
```

```
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:43:18 2020 MST
example.com> exitexample.com:rtestuser 53] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:fc:01
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet6 fe80::250:56ff:fe87:a646%lagg0 prefixlen 64 scopeid 0x7
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        groups: lagg
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
example.com:rtestuser 54]
```

Fermeture de l'interface P1

P1 et T1 sont jumelés et nommés DP1. En arrêtant P1, T1 deviendra actif. Dans l'exemple suivant, recherchez l'interface lagg0.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
1. DP1:
        Backup (T1) Standby, Link is up
        Primary (P1) Active, Link is up
2. DP2:
        Backup (T2) Standby, Link is up
        Primary (P2) Active, Link is up

Choose the operation you want to perform:
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com>
example.com> exit

example.com:rtestuser 115] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
```

```
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xffffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xffffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 116]
example.com:rtestuser 116] ifconfig nic1 down
example.com:rtestuser 117] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
```

```
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=1<MASTER>
        laggport: nic3 flags=4<ACTIVE>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 118]
```

Ouverture de l'interface P1

```
example.com:rtestuser 118] ifconfig nic1 up
example.com:rtestuser 119] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
```

```
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
```

```
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 120]
example.com:rtestuser 120]
```

Directives pour la configuration de l'appairage de cartes réseau

M2, Data1 et Data2 ne peuvent pas être utilisés comme adresse principale ou secondaire ou configurés avec une adresse IP.

Tableau 2 :

Ports	Configuré comme adresse IP	Action	Que faire?	Routage fractionné activé	
				Primaire	Secondaire
P1 (Proxy)	Oui	Activé	Connectez P1 au réseau pour le trafic entrant et sortant.	Vous pouvez sélectionner P1 comme principal pour l'appairage de cartes réseau **Remarque** Si vous sélectionnez P2 comme adresse principale, vous devez supprimer l'adresse IP de P1.	P2, T1, T2
P1 + P2 (Proxy)	Oui	Activé	Connectez P1 au réseau interne et P2 à Internet.	Si vous sélectionnez P2 comme adresse principale et P1 comme adresse secondaire, vous devez supprimer l'adresse IP de P1. Vous serez invité à supprimer l'adresse IP pendant l'appairage des cartes réseau.	T1, T2

Ports	Configuré comme adresse IP	Action	Que faire?	Routage fractionné activé	
				Primaire	Secondaire
T1 (Supervision du trafic)	Non	Dérivateur duplex	Un câble pour tout le trafic entrant et sortant.	S.O.	S.O.
T1 + T2 (Supervision du trafic)	Oui	Dérivateur simple	Un câble pour tous les paquets destinés à Internet (T1) et un câble pour tous les paquets provenant d'Internet (T2).	S.O.	S.O.

Remarque Si vous choisissez de supprimer l'adresse IP pour P1, P1 ne sera pas configuré sous le routage fractionné. Lorsqu'une adresse IP est attribuée pour P2 ou pour la paire de cartes réseau créée, le routage fractionné est activé avec P2 configuré seulement. L'interface d'agrégation de liens (LAGG) ne s'affiche pas tant que l'adresse IP n'est pas attribuée à la carte réseau principale (p2) ou à la paire de cartes réseau. Une fois l'adresse IP attribuée à la carte réseau principale (p2) ou à la paire de cartes réseau, l'interface LAGG est créée.

Configuration des groupes de basculement à des fins de haute disponibilité

À l'aide du protocole CARP (Common Address Redundancy Protocol), les Secure Web Appliance permettent à plusieurs hôtes de votre réseau de partager une adresse IP, fournissant une redondance IP pour assurer la haute disponibilité des services fournis par ces hôtes.

Le basculement est disponible uniquement pour le service proxy. Le proxy se lie automatiquement à l'interface de basculement lors de la création du groupe de basculement. Ainsi, si le proxy tombe en panne pour une raison quelconque, le basculement est déclenché.

Dans CARP, il existe trois états pour un hôte :

- primary : il ne peut y avoir qu'un seul hôte principal dans chaque groupe de basculement
- backup
- init

L'hôte principal du groupe de basculement CARP envoie des annonces régulières au réseau local pour que les hôtes de sauvegarde sachent qu'il est toujours actif. (Cet intervalle d'avertissement est configurable sur la Secure Web Appliance). Si les hôtes de sauvegarde ne reçoivent pas d'annonce du serveur principal pendant la période spécifiée (parce que le proxy est en panne, que le Secure Web Appliance est en panne ou qu'il est déconnecté du réseau), le basculement est déclenché et un des sauvegardes assumeront les fonctions de principal.

Les annonces de l'hôte principal Secure Web Appliance n'atteignent pas les hôtes de sauvegarde restants dans les conditions suivantes :

- Indisponibilité du réseau ou de l'interface
- Intégrité et disponibilité du système d'exploitation

Note Désactivez l'apprentissage IP du plan de données dans l'infrastructure axée sur l'application (ACI) pour utiliser la fonctionnalité Secure Web Appliance haute disponibilité.

Note Vous ne pouvez pas utiliser la haute disponibilité comme méthode d'équilibrage de la charge entre les appliances. Utilisez WCCP ou un équilibreur de charge matérielle pour équilibrer la charge du trafic entre les appliances.

Les configurations suivantes entraînent les basculements à haute disponibilité :

- Ajouter, supprimer ou mettre à jour le domaine d'authentification
- Ajouter, supprimer ou mettre à jour les paramètres ISE
- Ajouter ou mettre à jour le certificat HTTPS
- Mettre à jour le niveau de journalisation (journal du proxy)
- Mettre à jour le paramètre de redirection transparente
- Activer, désactiver ou mettre à jour le proxy FTP
- Activer, désactiver ou mettre à jour le proxy SOCKS
- Ajouter ou modifier le fichier PAC
- Ajouter ou supprimer l'interface de l'appliance
- Ajouter ou mettre à jour des groupes de basculement
- Activer ou désactiver le proxy en amont
- Activer ou désactiver WTT (dérivation du trafic Web)

Ajouter un groupe de basculement

Before you begin

- Identifiez une adresse IP virtuelle qui sera utilisée exclusivement pour ce groupe de basculement. Les clients utiliseront cette adresse IP pour se connecter au groupe de basculement en mode proxy de transfert explicite.
- Configurez toutes les appliances du groupe de basculement avec des valeurs identiques pour les paramètres suivants :

- Failover Group ID (ID du groupe de basculement)
- Hostname (Nom d'hôte)
- Virtual IP Address (Adresse IP virtuelle)

- Si vous configurez cette fonctionnalité sur une appliance virtuelle, assurez-vous que le commutateur virtuel et les interfaces virtuelles spécifiques à chaque appliance sont configurés pour utiliser le mode promiscuité. Pour en savoir plus, consultez la documentation de votre hyperviseur virtuel.

Étape 1 Choisissez **Network > High Availability** (Réseau > Haute disponibilité).

Étape 2 Cliquez sur **Add Failover Group** (Ajouter un groupe de basculement).

Étape 3 Saisissez une valeur pour **Failover Group ID** (ID de groupe de basculement) comprise entre 1 et 255.

Étape 4 (Facultatif) Saisissez une description.

Étape 5 Renseignez l'option **Hostname** (Nom d'hôte), par exemple, www.exemple.com.

Étape 6 Renseignez l'option **Virtual IP Address and Netmask** (Adresse IP virtuelle et le masque réseau), par exemple 10.0.0.3/24 (IPv4) ou 2001:420:80:1::5/32 (IPv6).

Étape 7 Choisissez une option dans le menu **Interface**. L'option **Select Interface Automatically** (Sélectionner une interface automatiquement) permet de sélectionner l'interface en fonction de l'adresse IP que vous avez fournie.

Note Si vous ne sélectionnez pas l'option **Select Interface Automatically** (Sélectionner une interface automatiquement), vous devez choisir une interface dans le même sous-réseau que l'adresse IP virtuelle que vous avez fournie.

Étape 8 Choisissez la priorité. Cliquez sur **Primary** (Principal) pour régler la priorité sur 255. Vous pouvez également sélectionner **Backup** (Sauvegarde) et saisir une priorité comprise entre 1 (la plus basse) et 254 dans le champ **Priority** (Priorité).

Étape 9 (Facultatif). Pour activer la sécurité pour le service, cochez la case **Enable Security for Service** (Activer la sécurité pour le service) et saisissez une chaîne de caractères qui sera utilisée comme secret partagé dans les champs **Shared Secret** (Secret partagé) et **Retype Shared Secret** (Retaper le secret partagé).

Note Le secret partagé, l'adresse IP virtuelle et l'ID du groupe de basculement doivent être les mêmes pour toutes les appliances du groupe de basculement.

Étape 10 Saisissez le délai en secondes (1 à 255) entre l'annonce de la disponibilité par les hôtes dans le champ **Advertisement Interval** (Intervalle d'annonce).

Étape 11 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Problèmes de basculement, on page 638

Modifier les paramètres globaux haute disponibilité

Étape 1 Choisissez **Network > High Availability** (Réseau > Haute disponibilité).

Étape 2 Dans la zone **High Availability Global Settings** (Paramètres globaux haute disponibilité), cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans le menu **Failover Management** (Gestion des basculements), choisissez une option.

- **Preemptive** (Préemptif) : l'hôte ayant la priorité la plus élevée prendra le contrôle lorsqu'il est disponible.
- **Non-preemptive** (Non préemptif) : l'hôte qui a le contrôle conserve le contrôle même si un hôte de priorité plus élevée devient disponible.

Étape 4 Cliquez sur **Submit** (Soumettre). Vous pouvez également cliquer sur **Cancel** (Annuler) pour abandonner vos modifications.

Afficher l'état des groupes de basculement

Choisissez **Network > High Availability** (Réseau > Haute disponibilité). La zone Failover Groups (Groupes de basculement) affiche le groupe de basculement actuel. Vous pouvez cliquer sur **Refresh Status** (Actualiser l'état) pour mettre à jour l'affichage. Vous pouvez également afficher les détails du basculement en sélectionnant **Network > Interfaces** (Réseau > Interfaces) ou **Report > System Status** (Rapport > État du système).

Utilisation de l'interface de données P2 pour les données de proxy Web

Par défaut, le proxy Web n'écoute pas les demandes sur P2, même lorsqu'il est activé. Cependant, vous pouvez configurer P2 pour qu'il écoute les données du proxy Web.

Note Si vous active P2 pour qu'il écoute les demandes des clients à l'aide de la commande d'interface de ligne de commande `advancedproxyconfig` > `miscellaneous`, vous pouvez choisir d'utiliser P1 ou P2 pour le trafic sortant. Pour utiliser P1 pour le trafic sortant, modifiez la voie de routage par défaut pour le trafic de données afin de préciser la prochaine adresse IP à laquelle l'interface P1.

Before you begin

Activez P2 (vous devez également activer P1, si ce n'est déjà fait) (voir Activation ou modification des interfaces réseau, on page 27).

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `advancedproxyconfig` > `miscellaneous` pour accéder à la zone requise.

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
```

```
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

Étape 3 []> **miscellaneous**

Étape 4 Appuyez sur **Enter** (Entrée) après chaque question jusqu'à la question :

`Do you want proxy to listen on P2?` (Voulez-vous que le proxy écoute sur P2?)

Saisissez « **Y** » (Oui) en réponse à cette question.

Étape 5 Appuyez sur **Enter** (Entrée) après les autres questions.

Étape 6 Validez vos modifications.

What to do next

Thèmes connexes

- Connecter l'appliance, on page 13.
- Configuration des routages de trafic TCP/IP, on page 43.
- Configuration de la redirection transparente, on page 46

Configuration des routages de trafic TCP/IP

Les voies de routage sont utilisées pour déterminer où envoyer (ou acheminer) le trafic réseau. Secure Web Appliance achemine les types de trafic suivants :

- **Trafic de données.** Trafic généré par les utilisateurs finaux qui naviguent sur le Web traité par le proxy Web .
- **Trafic de gestion.** Trafic créé par la gestion de l'appliance au moyen de l'interface Web et trafic que l'appliance crée pour les services de gestion, tels que les mises à niveau d'AsyncOS, les mises à jour de composants, DNS, l'authentification, etc.

Par défaut, les deux types de trafic utilisent les voies de routage définies pour toutes les interfaces réseau configurées. Cependant, vous pouvez choisir de fractionner le routage, de sorte que le trafic de gestion utilise une table de routage de gestion et le trafic de données utilise une table de routage de données. Les deux types de répartition du trafic sont répartis comme suit :

Trafic de gestion	Trafic de données
• IU Web • SSH • SNMP • Authentification NTLM (avec contrôleur de domaine) • Syslogs • FTP push • DNS (configurable) • Clé de mise à jour, de mise à niveau ou de fonctionnalité (configurable)	• HTTP • HTTPS • FTP • Négociation WCCP • Demande ICAP avec serveur DLP externe • DNS (configurable) • Clé de mise à jour, de mise à niveau ou de fonctionnalité (configurable) • Authentification LDAP/NTLM avec contrôleur de domaine (configurable)

Le nombre de sections sur la page **Network** > **Routes** (Réseau > Voies de routage) est déterminé par l'activation ou non du routage fractionné :

- **Sections de configuration de routage distinctes pour le trafic de gestion et de données** (routage fractionné activé). Lorsque vous utilisez l'interface de gestion pour le trafic de gestion uniquement [l'option **Restrict M1 port to appliance management services only** (Restreindre le port M1 aux services de gestion de l'appliance uniquement) est activé], cette page comprend deux sections pour la saisie des voies de routage, une pour le trafic de gestion et l'autre pour le trafic de données.
- **Section de configuration de routage pour tout le trafic** (routage fractionné non activé). Lorsque vous utilisez l'interface de gestion pour le trafic de gestion et de données [l'option **Restrict M1 port to appliance management services only** (Restreindre le port M1 aux services de gestion d'appliances uniquement) est désactivée], cette page comprend une section pour la saisie des voies de routages pour tout le trafic sortant de Secure Web Appliance, tant le trafic de gestion et que le trafic de données.

Note Une passerelle de routage doit résider sur le même sous-réseau que l'interface de gestion ou de données sur laquelle elle est configurée. Si plusieurs ports de données sont activés, le proxy Web envoie les transactions sur l'interface de données qui se trouve sur le même réseau que la passerelle par défaut configurée pour le trafic de données.

Trafic des services sortants

Secure Web Appliance utilise également les interfaces de gestion et de données pour acheminer le trafic sortant pour des services tels que le DNS, les mises à niveau logicielles, NTP et le trafic de données Traceroute. Ces paramètres doivent être configurés pour chaque service individuellement, en choisissant la voie de routage utilisée pour le trafic sortant. Par défaut, l'interface de gestion est utilisée pour tous les services.

Thèmes connexes

- Pour activer le routage fractionné du trafic de gestion et de données, consultez Activation ou modification des interfaces réseau, on page 27.

Modification de la voie de routage par défaut

Étape 1 Choisissez **Network > Routes** (Réseau > Voies de routage).

Étape 2 Cliquez sur **Default Route** (Voie de routage par défaut) dans le tableau de gestion ou de données, selon les besoins (ou sur le tableau combiné Gestion/données si le routage fractionné n'est pas activé).

Étape 3 Dans la colonne Gateway (passerelle), entrez l'adresse IP du système informatique sur le prochain saut du réseau connecté à l'interface réseau que vous modifiez.

Étape 4 Envoyez et validez vos modifications.

Ajout d'une voie de routage

Étape 1 Choisissez **Network > Routes** (Réseau > Voies de routage).

Étape 2 Cliquez sur le bouton **Add Route** (Ajouter une voie de routage) correspondant à l'interface pour laquelle vous créez la voie de routage.

Étape 3 Entrez un nom, un réseau de destination et une passerelle.

Étape 4 Envoyez et validez vos modifications.

Enregistrement et chargement des tableaux de routage

Choisissez **Network > Routes** (Réseau > Voies de routage).

Pour enregistrer une table de routage, cliquez sur **Save Route Table** (Enregistrer la table de routage) et indiquez l'emplacement d'enregistrement du fichier.

Pour charger une table de routage enregistrée, cliquez sur **Load Route Table** (Charger la table de routage), accédez au fichier, ouvrez-le, puis envoyez et validez vos modifications.

Note Lorsque l'adresse de destination se trouve sur le même sous-réseau que l'une des interfaces réseau physiques, AsyncOS envoie les données à l'aide de l'interface réseau du même sous-réseau. Il ne consulte pas les tables de routage.

Suppression d'une voie de routage

Étape 1 Choisissez **Network > Routes** (Réseau > Voies de routage).

Étape 2 Cochez la case dans la colonne Delete (Supprimer) de la voie de routage appropriée.

Étape 3 Cliquez sur **Delete** (Supprimer) et confirmez**.**

Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Activation ou modification des interfaces réseau, on page 27.

Configuration de la redirection transparente

Spécification d'un périphérique de redirection transparente

Before you begin

Connectez l'appliance à un commutateur de la couche 4 ou à un routeur WCCP v2.

Étape 1 Choisissez **Network > Transparent Redirection** (Réseau > Redirection transparente).

Étape 2 Cliquez sur **Edit Device** (Modifier le périphérique).

Étape 3 Choisissez le type de périphérique qui redirige de manière transparente le trafic vers l'appliance dans la liste déroulante Type : **Layer 4 Switch (Commutateur de la couche 4) ou No Device** (Aucun périphérique) ou **WCCP v2 Router** (Routeur WCCP v2).

Étape 4 Envoyez et validez vos modifications.

Étape 5 Pour les périphériques WCCP v2, procédez comme suit :

a) Configurez l'appareil WCCP en vous référant à la documentation correspondante.

b) Dans la page Transparent Redirection (Redirection transparente) de Secure Web Appliance, cliquez sur **Add Service** (Ajouter un service) pour ajouter un service WCCP, comme décrit dans Ajout et modification d'un service WCCP, on page 48.

c) Si l'usurpation d'adresses IP est activée sur l'appliance, créez un deuxième service WCCP.

What to do next

Thèmes connexes

- Connecter l'appliance, on page 13.
- Configuration des services WCCP, on page 47.

Utilisation d'un commutateur de couche 4

Si vous utilisez un commutateur de couche 4 pour la redirection transparente, selon sa configuration, vous devrez peut-être configurer quelques options supplémentaires sur Secure Web Appliance.

- En général, n'activez pas l'usurpation d'adresses IP; Si vous usurpez des adresses IP en amont, vous risquez de créer une boucle de routage asynchrone.
- Dans la page Edit Web Proxy Settings (Modifier les paramètres de proxy Web) [Security Services > Web Proxy (Services de sécurité > Proxy Web)], cochez la case **Enable Identification of Client IP Addresses using X-Forwarded-For** (Activer l'identification des adresses IP des clients à l'aide de

X-Forwarded-For) dans la section **Use Received Headers** (Utiliser les en -têtes reçus) (paramètres avancés). Ajoutez ensuite une ou plusieurs adresses IP de sortie à la liste **Trusted Downstream Proxy or Load Balancer** (Proxys en aval approuvés ou équilibreur de charge).

- Vous pouvez également utiliser la commande d'interface de ligne de commande `advancedproxyconfig > miscellaneous` pour configurer les paramètres suivants liés au proxy, au besoin :
  - `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)? [Voulez-vous que le proxy réponde aux contrôles de l'intégrité des commutateurs de la couche 4 (toujours activés si WSA est en mode transparent sur la couche 4)?]` – Saisissez Y (Oui) si vous souhaitez permettre à Secure Web Appliance de répondre aux contrôles de l'intégrité.
  - `Would you like proxy to perform dynamic adjustment of TCP receive window size?` (Voulez-vous que le proxy effectue un ajustement dynamique de la taille de la fenêtre de réception TCP?) – Saisissez Y (Oui) par défaut dans la plupart des cas; saisissez N si vous avez un autre périphérique proxy en amont de Secure Web Appliance.
  - `Do you want to pass HTTP X-Forwarded-For headers?` (Voulez-vous transmettre les en-têtes HTTP X-Forwarded-For?) – Inutile, sauf s'il existe une exigence en amont pour les en-têtes X-Forwarded-For (XFF).
  - `Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?` (Voulez-vous que le proxy consigne les valeurs des en-têtes X-Forwarded-For à la place des adresses IP de connexion entrante?) – Pour faciliter le dépannage, vous pouvez saisir Y (Oui); les adresses IP des clients seront affichées dans les journaux d'accès.
  - `Would you like the proxy to use client IP addresses from X-Forwarded-For headers?` (Voulez-vous que le proxy utilise les adresses IP clientes des en-têtes X-Forwarded-For?) Encore une fois, pour faciliter la configuration des politiques et la production de rapports, vous pouvez saisir Y (Oui).
- Si vous utilisez des en-têtes X-Forwarded-For (XFF), ajoutez `%f` à l'abonnement aux journaux d'accès afin de journaliser les en-têtes XFF. Pour le format des journaux W3C, ajoutez `cs(X-Forwarded-For)`.

Configuration des services WCCP

Un service WCCP est une configuration d'appliance qui définit un groupe de services pour un routeur WCCP v2. Il comprend des informations telles que l'ID de service et les ports utilisés. Les groupes de services permettent à un proxy Web d'établir la connectivité avec un routeur WCCP et de gérer le trafic redirigé à partir du routeur.

Si la vérification de l'intégrité du proxy WCCP est activée, le démon WCCP de Secure Web Appliance envoie un message de vérification de l'intégrité du proxy (demande du client xmlRPc) au serveur xmlRPc qui s'exécute sur le proxy Web toutes les 10 secondes. Si le proxy est opérationnel, le service WCCP reçoit une réponse du proxy et la commande Secure Web Appliance envoie un message « here je suis » (HIA) aux routeurs compatibles avec WCCP spécifiés toutes les 10 secondes. Si le service WCCP ne reçoit pas de réponse du proxy, les messages HIA ne sont pas envoyés aux routeurs WCCP.

Après avoir raté trois messages HIA consécutifs à un routeur WCCP, le routeur supprime le Secure Web Appliance de son groupe de services et le trafic n'est plus acheminé vers le Secure Web Appliance.

Vous pouvez utiliser la commande d'interface de ligne de commande `advancedproxyconfig > miscellaneous > Do you want to enable WCCP proxy health check?` (Voulez-vous activer la vérification de l'intégrité du proxy WCCP?) pour activer et désactiver les messages de vérification de l'intégrité du proxy; le contrôle de l'intégrité est désactivé par défaut.

Note Le service WCCPv2 fonctionne avec les réseaux IPv4 et IPv6. Un maximum de 15 groupes de services peuvent être configurés sur une seule appliance. Chaque groupe de services du routeur WCCP peut contenir jusqu'à 32 appliances. Le service WCCPv2 est également utilisé pour le mécanisme d'équilibrage de la charge afin de réduire la surcharge du moteur de contenu et le blocage de données.

Note La configuration de WCCP et de la haute disponibilité sur la même appliance n'est pas prise en charge. Si ces paramètres sont configurés, Secure Web Appliance ne fonctionnera pas comme prévu.

- À propos de l'équilibrage des charges WCCP, on page 48
- Ajout et modification d'un service WCCP, on page 48
- Création de services WCCP pour l'usurpation d'adresses IP, on page 52

À propos de l'équilibrage des charges WCCP

Le paramètre **Assignment Weight** (Pondération des affectations) dans la définition de service WCCP est utilisé pour équilibrer la charge sur ce Secure Web Appliance lorsqu'il fonctionne en tant que membre d'un groupe WCCP ou d'un groupe de services. Cette pondération représente la proportion du trafic total WCCP qui peut être envoyée vers ce Secure Web Appliance pour traitement.

L'ajustement de la pondération des affectations n'est requis que lorsque différents types d'appliances de passerelle sont membres du même groupe WCCP et que vous devez détourner une plus grande partie du trafic vers les appliances plus puissantes.

Remarque Tous les Secure Web Appliance qui sont membres d'un groupe WCCP doivent exécuter une version d'AsyncOS qui prend en charge la pondération des affectations pour pouvoir bénéficier de l'équilibrage des charges WCCP.

Remarque WCCP équilibre la charge du trafic transparent pour un maximum de 32 appliances. Il équilibre le flux du trafic en fonction du hachage ou du masque et ceux-ci sont pondérés lorsque plusieurs modèles d'appliances sont connectés au réseau. Sans temps d'arrêt, vous pouvez ajouter et supprimer des appliances du groupe de services. Toutefois, si vous utilisez ou prévoyez d'utiliser plus de 8 appliances, nous vous recommandons d'avoir un équilibreur de charge dédié.

Consultez Ajout et modification d'un service WCCP, à la page 48 pour de plus amples renseignements sur le paramètre **Assignment Weight** (Pondération des affectations).

Ajout et modification d'un service WCCP

Before you begin

Configurez l'appliance pour utiliser un routeur WCCP v2 (voir Spécification d'un périphérique de redirection transparente, on page 46).

Étape 1 Choisissez **Network > Transparent Redirection** (Réseau > Redirection transparente).

Étape 2 Cliquez sur **Add Service** (Ajouter un service) ou, pour modifier un service WCCP, cliquez sur le nom du service WCCP dans la colonne Service Profile Name (Nom du profil de service).

Étape 3 Configurez les options du WCCP comme décrit :

Options du service WCCP	Description
Service Profile Name (Nom du profil du service)	Le nom du service WCCP. **Note** Si vous laissez ce champ vide et choisissez un service standard (voir ci-dessous), le nom « web_cache » est automatiquement attribué ici.
Service	Le type de groupe de services pour le routeur. Choisissez parmi : **Standard service** (Service standard). Ce type de service reçoit un ID fixe de zéro, une méthode de redirection fixe *par port de destination* et un port de destination fixe de 80. Vous ne pouvez créer qu'un seul service standard. Si un service standard existe déjà sur l'appliance, cette option est grisée. **Dynamic service** (Service DNS). Ce type de service vous permet de définir un ID personnalisé, des numéros de port et des options de redirection et d'équilibrage de la charge. Saisissez les mêmes paramètres que vous avez saisis pour le service dynamique sur le routeur WCCP. Si vous créez un service dynamique, entrez les informations suivantes : • **Service ID(** (ID du service). Vous pouvez entrer n'importe quel nombre entre 0 et 255 dans le champ Dynamic Service ID. Cependant, notez que vous ne pouvez pas configurer plus de 15 groupes de services sur cette appliance. • **Port number(s)** [Numéro(s) de port]. Saisissez jusqu'à huit numéros de port pour le trafic à rediriger dans le champ Port Numbers (Numéros de port). • **Redirection basis** (Base de redirection). Choisissez de rediriger le trafic en fonction du port de source ou de destination. Le port de destination est défini par défaut. **Note** Pour configurer le FTP natif avec une redirection transparente et une usurpation d'adresses IP, choisissez Redirect basé sur le port source (chemin de retour) et définissez le port source sur 13007. • **Load balancing basis** (Base d'équilibrage de la charge). Lorsque le réseau utilise plusieurs Secure Web Appliance, vous pouvez choisir la façon de répartir les paquets entre les appliances. Vous pouvez distribuer des paquets en fonction de l'adresse du serveur ou du client. Lorsque vous choisissez l'adresse du client, les paquets d'un client sont toujours distribués vers la même appliance. L'adresse par défaut est l'adresse du serveur.
Router IP Addresses (Adresses IP du routeur)	L'adresse IPv4 ou IPv6 d'un ou de plusieurs routeurs compatibles avec WCCP. Utilisez l'adresse IP unique de chaque routeur; vous ne pouvez pas entrer une adresse de multidiffusion. Vous ne pouvez pas combiner des adresses IPv4 et IPv6 dans un groupe de services.

Options du service WCCP	Description
Router Security (Sécurité des routeurs)	Cochez la case **Enable Security for Service** (Activer la sécurité pour le service) afin d'exiger une phrase secrète pour ce groupe de services. Si cette option est activée, chaque appliance et routeur WCCP utilisant le groupe de services doit utiliser la même phrase secrète. Saisissez et confirmez la phrase secrète à utiliser.

Options du service WCCP	Description
Advanced (Niveau avancé)	**Load-Balancing Method** (Méthode d'équilibrage de la charge). Cela détermine la façon dont le routeur effectue l'équilibrage de la charge des paquets entre plusieurs Secure Web Appliance. Choisissez parmi : • **Allow Mask Only** (Autoriser le masque uniquement). Les routeurs WCCP prennent des décisions à l'aide du matériel du routeur. Cette méthode peut augmenter les performances du routeur par rapport à la méthode de hachage. Cependant, tous les routeurs WCCP ne prennent pas en charge l'affectation de masque. (IPv4 uniquement.) • **Allow Hash Only** (Autoriser le hachage uniquement). Cette méthode s'appuie sur une fonction de hachage pour prendre des décisions de redirection. Cette méthode peut être moins efficace que la méthode du masque, mais c'est peut-être la seule option prise en charge par le routeur. (IPv4 et IPv6.) • **Allow Hash or Mask** (Autoriser le hachage ou le masquage). Permet à AsyncOS de négocier une méthode avec le routeur. Si le routeur prend en charge le masque, AsyncOS utilise le masquage, sinon le hachage est utilisé. **Mask Customization** (Personnalisation du masque). Si vous sélectionnez Allow Mask Only (Autoriser le masque uniquement) ou Allow Hash ou Mask (Autoriser le hachage ou le masquage), vous pouvez personnaliser le masquage ou préciser le nombre de bits : • **Custom mask (max 6 bits)** [Masque personnalisé (maximum 6 bits)]. Vous pouvez préciser le masque. L'interface Web affiche le nombre de bits associés au masque que vous fournissez. Vous pouvez utiliser jusqu'à cinq bits pour un routeur IPv4 ou six bits pour un routeur IPv6. • **System generated mask** (Masque généré par le système). Vous pouvez laisser le système générer un masque pour vous. Vous pouvez également spécifier le nombre de bits pour le masque généré par le système, entre un et cinq bits. **Assignment Weight** (Pondération des affectations). La pondération du WCCP pour ce Secure Web Appliance; les valeurs valides sont comprises entre zéro et 255. Cette pondération représente la proportion du trafic total qui peut être envoyée à ce Secure Web Appliance pour traitement en tant que membre d'un groupe de services WCCP. La valeur zéro signifie que ce Secure Web Appliance fera partie du groupe de services, mais ne recevra aucun trafic redirigé du routeur. Consultez À propos de l'équilibrage des charges WCCP, on page 48 pour obtenir de plus amples renseignements. **Forwarding method** (Méthode de transfert.) Cette méthode permet de transporter les paquets redirigés du routeur au proxy Web. **Return Method** (Méthode de retour). Cette méthode permet de transporter les paquets redirigés du proxy Web au routeur.

Options du service WCCP	Description
	Les méthodes de transfert et de retour utilisent l'un des types de méthode suivants : • **Layer 2 (L2)** [Couche 2 (L2)]. Cette méthode redirige le trafic de la couche 2 en remplaçant l'adresse MAC de destination du paquet par l'adresse MAC du proxy Web cible. La méthode L2 fonctionne au niveau matériel et offre généralement les meilleures performances. Cependant, tous les routeurs WCCP ne prennent pas en charge le transfert L2. De plus, les routeurs WCCP n'autorisent la négociation L2 qu'avec un Secure Web Appliance directement (physiquement) connecté. • **Generic Routing Encapsulation (GRE)** [GRE (Generic Routing Encapsulation)]. Cette méthode redirige le trafic vers la couche 3 en encapsulant le paquet IP avec un en-tête GRE et un en-tête de redirection. GRE fonctionne au niveau logiciel, ce qui peut avoir une incidence sur les performances. • **L2 or GRE** (L2 ou GRE). Avec cette option, l'appliance utilise la méthode que le routeur dit prendre en charge. Si le routeur et l'appliance prennent en charge la couche 2 et GRE, l'appliance utilise la couche 2. Si le routeur n'est pas connecté directement à l'appliance, vous devez choisir GRE.

Étape 4 Envoyez et validez vos modifications.

Création de services WCCP pour l'usurpation d'adresses IP

Étape 1 Si vous avez activé l'usurpation d'adresses IP sur le proxy Web, créez deux services WCCP. Créez un service WCCP standard ou créez un service WCCP dynamique qui redirige le trafic en fonction des ports de destination.

Étape 2 Créez un service WCCP dynamique qui redirige le trafic en fonction des ports source.

Utilisez les mêmes numéros de port, l'adresse IP du routeur et les paramètres de sécurité du routeur que pour le service créé à l'étape 1.

Note
- Cisco suggère d'utiliser un numéro d'ID de service compris entre 90 et 97 pour le service WCCP utilisé pour le chemin de retour (en fonction du port source).
- Configurez correctement les adresses IP frauduleuses lorsque vous définissez les méthodes d'équilibrage de charge WCCP **« Allow Mask Only »** (Autoriser le masque uniquement) ou **« Allow Hash or Mask »** (Autoriser le hachage ou le masque) pour répartir le trafic entre plusieurs appliances. La configuration d'une adresse IP usurpée doit assurer un routage approprié du trafic entre le routeur WCCP et Secure Web Appliance.

What to do next

Thèmes connexes

- Cache du proxy Web, on page 77.

Augmentation de la capacité de l'interface à l'aide de VLAN

Vous pouvez configurer un ou plusieurs VLAN pour augmenter le nombre de réseaux auxquels Cisco Secure Web Appliance peut se connecter au-delà du nombre d'interfaces physiques incluses.

Les VLAN se présentent comme des « ports de données » dynamiques étiquetés au format : « VLAN DDDD » où « DDDD » est l'ID et un entier comprenant jusqu'à 4 chiffres (VLAN 2 ou VLAN 4094, par exemple). AsyncOS prend en charge jusqu'à 30 VLAN.

Un port physique n'a pas besoin qu'une adresse IP soit configurée pour figurer dans un VLAN. Le port physique sur lequel un VLAN est créé peut avoir une adresse IP qui recevra le trafic non VLAN, de sorte que vous pouvez avoir le trafic VLAN et non VLAN sur la même interface.

Des VLAN peuvent être créés sur l'interface de gestion en utilisant M1, P1 pour les ports de données internes et P2 pour les ports de données externes.

Configuration et gestion des VLAN

Vous pouvez créer, modifier et supprimer des VLAN à l'aide de la commande `etherconfig`. Une fois créé, un VLAN peut être configuré au moyen de la commande `interfaceconfig` dans l'interface de ligne de commande.

Note Chaque fois que vous apportez des modifications à une configuration VLAN, veillez à redémarrer l'appliance.

Exemple 1 : création d'un nouveau VLAN

Dans cet exemple, deux VLAN sont créés (appelés VLAN 31 et VLAN 34) sur le port P1 :

Note Ne créez pas de VLAN sur les interfaces T1 ou T2.

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Suivez les étapes illustrées.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 34
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
```

```
VLAN interfaces:
1. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN   31 (P1)
2. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
```

Étape 3 Validez vos modifications.

Exemple 2 : création d'une interface IP sur un VLAN

Dans l'exemple donné, une nouvelle interface IP est créée sur l'interface Ethernet VLAN 34.

Note Apporter des modifications à une interface peut fermer votre connexion à l'appliance.

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Suivez les étapes illustrées :

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> new
IP Address (Ex: 10.10.10.10):
[]> 10.10.31.10
Ethernet interface:
1. Management
2. P1
3. VLAN 31
4. VLAN   34
[1]> 4
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>
```

```
Hostname:
[]> v.example.com
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN   34 (10.10.31.10 on VLAN  34: v.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
example.com> commit
```

Étape 3 Validez vos modifications.

What to do next

Thèmes connexes

- Activation ou modification des interfaces réseau, on page 27.
- Configuration des routages de trafic TCP/IP, on page 43.

Nom de domaine de redirection et nom de domaine du système

Après avoir exécuté l'Assistant de configuration du système, le nom d'hôte système et le nom d'hôte de redirection sont identiques. Cependant, la modification du nom d'hôte du système à l'aide de la commande `sethostname` ne modifie pas le nom d'hôte de redirection. Par conséquent, les paramètres peuvent avoir des valeurs différentes.

AsyncOS utilise le nom d'hôte de redirection pour les notifications et les accusés de réception de l'utilisateur final.

Le nom d'hôte du système est le nom d'hôte complet utilisé pour identifier l'appliance dans les domaines suivants :

- Interface de ligne de commande (CLI)
- Alertes du système
- Lors de la formation du nom NetBIOS de l'ordinateur lorsque Secure Web Appliance rejoint un domaine Active Directory.

Le nom d'hôte du système ne correspond pas directement aux noms d'hôte d'interface et n'est pas utilisé par les clients pour se connecter à l'appliance.

Modification du nom de domaine de redirection

Étape 1 Dans l'interface utilisateur Web, accédez à **Network**>**Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur Edit Global Settings (Modifier les paramètres globaux).

Étape 3 Entrez une nouvelle valeur pour le nom d'hôte de redirection.

Modification du nom de domaine du système

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez la commande `sethostname` pour modifier le nom de Secure Web Appliance :

```
example.com> sethostname

example.com> hostname.com

example.com> commit
...
hostname.com>
```

Étape 3 Validez vos modifications.

Configuration des paramètres de l'hôte de relais SMTP

AsyncOS envoie régulièrement des courriels générés par le système, tels que des notifications, des alertes et des demandes à l'assistance client de Cisco. Par défaut, AsyncOS utilise les informations répertoriées dans l'enregistrement MX de votre domaine pour envoyer des courriels. Toutefois, si l'appliance ne peut pas atteindre directement les serveurs de messagerie répertoriés dans l'enregistrement MX, vous devez configurer au moins un hôte de relais SMTP sur l'appliance.

Note Si le Secure Web Appliance ne peut pas communiquer avec les serveurs de messagerie répertoriés dans l'enregistrement MX ou l'un des hôtes de relais SMTP configurés, il ne peut pas envoyer de courriels, et il écrit un message dans les fichiers journaux.

Vous pouvez configurer un ou plusieurs hôtes de relais SMTP. Lorsque vous configurez plusieurs hôtes de relais SMTP, AsyncOS utilise celui qui se trouve en tête de la liste des hôtes de relais SMTP disponibles. Si un hôte de relais SMTP n'est pas disponible, il essaie d'utiliser celui qui se trouve en dessous dans la liste.

Configuration d'un hôte de relais SMTP

Étape 1 Choisissez **Network > Internal SMTP Relay** (Réseau > Relais SMTP interne).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Renseignez les paramètres du relais SMTP interne.

Propriété	Description
Relay Hostname or IP Address (Nom d'hôte ou adresse IP à utiliser pour le relais SMTP)	Le nom d'hôte ou l'adresse IP à utiliser pour le relais SMTP

Propriété	Description
Port	Le port pour la connexion au relais SMTP. Si cette propriété est laissée vide, l'appliance utilise le port 25.
Routing Table to Use for SMTP (Tableau de routage à utiliser pour SMTP)	La table de routage associée à une interface réseau de dispositif, de gestion ou de données, à utiliser pour la connexion au relais SMTP. Choisissez l'interface qui se trouve sur le même réseau que le système de relais.

Étape 4 (Facultatif) Cliquez sur **Add Line** (Ajouter une ligne) pour ajouter des hôtes de relais SMTP supplémentaires.

Étape 5 Envoyez et validez vos modifications.

DNS Settings (paramètres DNS)

AsyncOS pour le Web peut utiliser les serveurs DNS racine Internet ou vos propres serveurs DNS. Lorsque vous utilisez les serveurs racine Internet, vous pouvez spécifier d'autres serveurs à utiliser pour des domaines spécifiques. Étant donné qu'un autre serveur DNS s'applique à un seul domaine, il doit faire autorité (fournir les enregistrements DNS définitifs) pour ce domaine.

Vous pouvez également spécifier des serveurs de noms DNS secondaires pour résoudre les requêtes non résolues par les serveurs de noms principaux. Les serveurs DNS secondaires ne sont pas utilisés comme serveurs DNS de basculement. Ils sont interrogés en fonction de la priorité, lorsque les serveurs DNS principaux renvoient les erreurs spécifiées dans Modification des paramètres DNS, on page 58.

Pour éviter les échecs d'authentification, assurez-vous que le nom de redirection d'authentification Secure Web Appliance est unique.

- DNS fractionné, on page 58
- Effacement du cache DNS, on page 58
- Modification des paramètres DNS, on page 58

Lignes directrices et limites relatives au DNS sécurisé

Remarque Secure DNS est désactivé par défaut.

Si vous activez Secure DNS :

- Vous devez utiliser le nom de domaine complet (FQDN) avec le nom d'hôte pour les domaines local et privé.
- Assurez-vous de configurer le serveur DNS avec DNSSec, car il n'y a pas de compatibilité ascendante. Ne pas le faire peut entraîner une réponse non valide avec un nom d'hôte non résolu.
- Les journaux du système ne s'affichent pas :
  - Détails du serveur des requêtes DNS de la racine d'Internet
  - Des informations détaillées sur les journaux de débogage et de suivi

- CNAME n’est pas mis en cache.
- Les réponses DNSSEC non valides n’ont pas été mises en cache.
- Le cache DNS est effacé lorsque le paramètre DNS sécurisé passe de désactivé à activé, et inversement.
- Assurez-vous de sélectionner **Load Network Settings** (Charger les paramètres réseau) pour charger la configuration Secure DNS.

DNS fractionné

AsyncOS prend en charge le DNS fractionné où les serveurs internes sont configurés pour des domaines spécifiques et les serveurs DNS externes ou racine sont configurés pour d’autres domaines. Si vous utilisez votre propre serveur interne, vous pouvez également indiquer les domaines d’exception et les serveurs DNS associés.

Effacement du cache DNS

Before you begin

Sachez que l’utilisation de cette commande peut dégrader temporairement les performances pendant le remplissage du cache.

Étape 1 Choisissez **Network > DNS** (Réseau > DNS).

Étape 2 Cliquez sur **Clear DNS Cache** (Effacer le cache DNS).

Modification des paramètres DNS

Étape 1 Choisissez **Network > DNS** (Réseau > DNS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Configurez les paramètres DNS selon les besoins.

Propriété	Description
Serveurs DNS principaux	**Use these DNS Servers** (Utilisez ces serveurs DNS). Le ou les serveurs DNS locaux que l'appliance peut utiliser pour résoudre les noms d'hôte. **Alternate DNS servers Overrides (Optional)** [Autres remplacements de serveurs DNS (facultatif)]. Serveurs DNS faisant autorité pour des domaines particuliers **Use the Internet's Root DNS Servers** (Utilisez les serveurs DNS racine d'Internet). Vous pouvez choisir d'utiliser les serveurs DNS racine d'Internet pour les recherches de service de nom de domaine lorsque l'appliance n'a pas accès aux serveurs DNS de votre réseau. **Note** Les serveurs DNS racine Internet ne résolvent pas les noms d'hôte locaux. Si vous avez besoin que l'appliance résolve les noms d'hôte locaux, vous devez utiliser un serveur DNS local ou ajouter les entrées statiques appropriées au DNS local à l'aide de l'interface de ligne de commande. Cela est également nécessaire pour accéder à la nouvelle interface Web.
Secondary DNS Servers (Serveurs DNS secondaires)	Le ou les serveurs DNS secondaires que l'appliance peut utiliser pour résoudre les noms d'hôte non résolus par les serveurs de noms principaux. **Note** Les serveurs DNS secondaires reçoivent des requêtes de nom d'hôte lorsque les serveurs DNS principaux renvoient les erreurs suivantes : • Pas d'erreur, aucune section de réponse reçue. • Le serveur n'a pas réussi à traiter la demande. Aucune section de réponse. • Erreur de nom, aucune section de réponse reçue. • Fonction non mise en œuvre. • Le serveur a refusé de répondre à la requête.
Routing Table for DNS Traffic (Table de routage du trafic DNS)	Indique l'interface par laquelle le service DNS acheminera le trafic.
IP Address Version Preference (Préférence de version de l'adresse IP)	Lorsqu'un serveur DNS fournit à la fois une adresse IPv4 et une adresse IPv6, AsyncOS utilise cette préférence pour choisir la version de l'adresse IP. **Note** AsyncOS ne respecte pas la préférence de version pour les demandes FTP transparentes.
Secure DNS (DNS sécurisé)	Cochez la case **Secure DNS** (DNS sécurisé) pour valider l'authentification de la réponse DNS reçue du serveur DNS. **Note** L'activation de Cisco Secure DNS augmente le temps de résolution.
Wait Before Timing out Reverse DNS Lookups (Attendre avant d'interrompre les recherches DNS inversées)	Le temps d'attente en secondes avant d'interrompre les recherches DNS inversées non réactives.

Propriété	Description
Domain Search List (Liste de recherche de domaine)	Liste de recherche de domaines DNS utilisée lorsqu'une demande est envoyée à un nom d'hôte nu (sans caractère « . »). Les domaines spécifiés seront essayés à tour de rôle, dans l'ordre saisi, pour voir si une correspondance DNS peut être trouvée pour le nom d'hôte et le domaine.

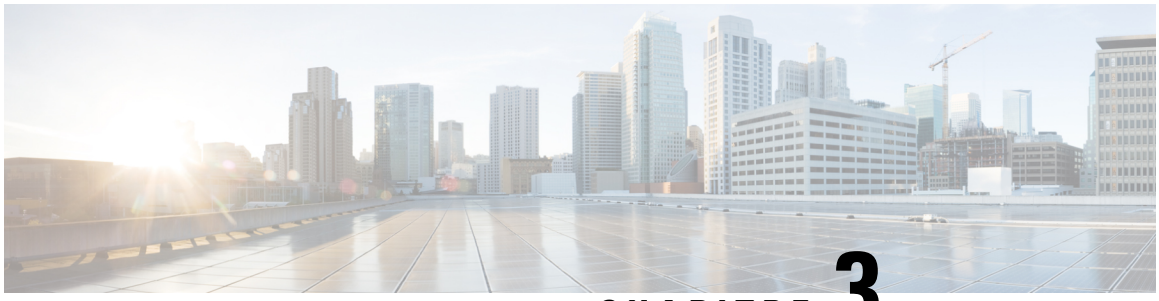
Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Configuration des routages de trafic TCP/IP, on page 43
- Versions d'adresses IP, on page 26

Résolution de problèmes de connexion, d'installation et de configuration



CHAPITRE 3

Connecter l'appliance à un proxy Cisco Cloud Web Security

Cette rubrique contient les sections suivantes :

Comment configurer et utiliser les fonctionnalités en mode Cloud Connector

L'utilisation des fonctionnalités incluses dans le sous-ensemble Cloud Connector est la même qu'en mode standard, sauf indication contraire. Voir Comparaison des modes de fonctionnement, on page 8 pour de plus amples informations.

Cette rubrique contient des liens vers des emplacements de cette documentation qui fournissent des informations sur quelques-unes des principales fonctionnalités de Secure Web Appliance communes au mode standard et au mode Cloud Web Security Connector. À l'exception des paramètres de configuration de Cloud Connector et des informations sur l'envoi de groupes d'annuaires dans le nuage, les informations pertinentes se trouvent dans d'autres sections du document.

Cette rubrique contient des informations sur la configuration de Cloud Web Security Connector qui ne s'appliquent pas au mode standard.

Ce document ne contient pas d'informations sur le produit Cisco Cloud Web Security. La documentation relative à Cloud Connector est disponible à l'adresse suivante :
http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

Déploiement en mode Cloud Connector

Lors de la configuration initiale de l'appliance, vous pouvez choisir de la déployer en mode Cloud Connector ou en mode standard. Vous pouvez également exécuter l'Assistant de configuration du système sur une appliance qui est actuellement déployée en mode standard pour la redéployer en mode Cloud Connector, si vous disposez des licences requises. L'exécution de l'Assistant de configuration du système remplace vos configurations existantes et supprime toutes les données existantes.

Le déploiement de l'appliance est identique en mode standard et en mode Cloud Security, sauf que les services de proxy Web et les services de supervision du trafic de la couche 4 ne sont pas disponibles en mode Cloud Web Security Connector.

Vous pouvez déployer Cloud Web Security Connector en mode de transfert explicite ou en mode transparent.

Pour modifier les paramètres de Cloud Connector après la configuration initiale, sélectionnez **Network** > **Cloud Connector** (Réseau > Cloud Connector).

Thèmes connexes

- Connexion, installation et configuration, on page 7

Configuration de Cloud Connector

Before you begin

Voir Activation de l'accès à l'interface Web sur les appliances virtuelles .

Étape 1 Accédez à l'Interface Web de Secure Web Appliance :

Saisissez l'adresse IPv4 de Secure Web Appliance dans un navigateur Internet.

La première fois que vous exécutez l'Assistant de configuration du système, utilisez l'adresse IPv4 par défaut :

`https://192.168.42.42:8443`

-ou-

`http://192.168.42.42:8080`

`192.168.42.42` étant l'adresse IPv4 par défaut, `8080` le paramètre du port d'administration par défaut pour HTTP et `8443` le port d'administration par défaut pour HTTPS.

Étape 2 Sélectionnez **System Administration > System Setup Wizard** (Administration système >Assistant de configuration du système).

Étape 3 Acceptez les conditions du contrat de licence.

Étape 4 Cliquez sur **Start Setup** (Commencer la configuration).

Étape 5 Configurez les paramètres système :

Paramètres	Description
Default System Hostname (Nom d'hôte du système par défaut)	Nom d'hôte complet de Secure Web Appliance.

Paramètres	Description
DNS Server(s) [Serveur(s) DNS]	Serveurs DNS racine Internet pour les recherches de services de noms de domaine. Voir aussi DNS Settings (paramètres DNS), on page 57.
NTP Server (Serveur NTP)	Serveur avec lequel synchroniser l'horloge système. La valeur par défaut est time.ironport.com.
Time Zone (Fuseau horaire)	Définit le fuseau horaire sur l'appliance de sorte que les horodatages dans les en-têtes des messages et les fichiers journaux soient corrects.

Étape 6 Sélectionnez **Cloud Web Security Connector** pour le mode de l'appliance.

Étape 7 Configurez les paramètres du Cloud Connector :

Paramètres	Description
Cloud Web Security Proxy Servers (Serveurs proxy Cloud Web Security)	Adresse du serveur proxy dans le nuage (CPS), par exemple, proxy1743.scansafe.net.
Failure Handling (Gestion des échecs)	Si AsyncOS ne parvient pas à se connecter à un proxy Cloud Web Security, sélectionnez **Connect directly** (Se connecter directement) pour vous connecter directement à Internet ou sélectionnez **Drop requests** (Abandonner les demandes).
Cloud Web Security Authorization Scheme (Schéma d'autorisation Cloud Web Security)	Méthode d'autorisation des transactions : • Adresse IPv4 publique de Secure Web Appliance • Clé d'autorisation incluse avec chaque transaction. Vous pouvez générer une clé d'autorisation dans le portail Cisco Cloud Web Security.

Étape 8 Configurez le câblage et les interfaces réseau :

Paramètres	Description
Ethernet Port (Port Ethernet)	Si vous configurez l'interface M1 pour le trafic de gestion uniquement, vous devez configurer l'interface P1 pour le trafic de données. Cependant, vous pouvez configurer l'interface P1 même lorsque l'interface M1 est utilisée à la fois pour la gestion et le trafic de données.
IP Address (Adresse IP)	Adresse IPv4 à utiliser pour gérer Secure Web Appliance.
Network Mask (Masque réseau)	Masque réseau à utiliser lors de la gestion de Secure Web Appliance sur cette interface réseau.
Hostname (Nom d'hôte)	Nom d'hôte à utiliser lors de la gestion de Secure Web Appliance sur cette interface réseau.

Étape 9 Configurez les voies de routage pour le trafic de gestion et de données :

Paramètres	Description
Default Gateway (Passerelle par défaut)	Adresse IPv4 par défaut de la passerelle à utiliser pour le trafic via l'interface de gestion et/ou de données.
Name (Nom)	Nom utilisé pour identifier la voie de routage statique.
Internal Network (Réseau interne)	Adresse IPv4 pour la destination de cette voie de routage sur le réseau.
Internal Gateway (Passerelle interne)	Adresse IPv4 de la passerelle pour cette voie de routage. Une passerelle de routage doit résider sur le même sous-réseau que l'interface de gestion ou de données sur laquelle elle est configurée.

Étape 10 Configurez les paramètres de connexion transparents :

Note Par défaut, le Cloud Connector est déployé en mode transparent, ce qui nécessite une connexion à un commutateur de couche 4 ou à un routeur WCCP version 2.

Paramètres	Description
Layer-4 Switch (Commutateur de couche 4) ou No Device (Aucun périphérique)	• Le Secure Web Appliance est connecté à un commutateur de couche 4. ou • Vous déploierez le Cloud Connector en mode de transfert explicite.
WCCP v2 Router (Routeur WCCP v2)	Le Secure Web Appliance est connecté à un routeur compatible avec WCCP version 2. Remarque : Une phrase secrète peut contenir jusqu'à sept caractères et est facultative.

Étape 11 Configurez les paramètres d'administration :

Paramètres	Description
Administrator Passphrase (Phrase secrète de l'administrateur)	Phrase secrète pour l'accès à Secure Web Appliance. La phrase secrète doit comporter au moins six caractères.
Email system alerts to (Alertes du système par e-mail à)	Adresse de messagerie à laquelle l'appliance envoie des alertes.
Send Email via SMTP Relay Host (Envoyer un e-mail par l'intermédiaire de l'hôte de relais SMTP)	(Facultatif) Nom d'hôte ou adresse d'un hôte de relais SMTP qu'utilise AsyncOS pour envoyer les messages par e-mail générés par le système. L'hôte de relais SMTP par défaut comprend les serveurs de messagerie répertoriés dans l'enregistrement MX. Le numéro de port par défaut est 25.
AutoSupport (AutoAssistance)	L'appliance peut envoyer des alertes système et un rapport d'état hebdomadaire à l'assistance client de Cisco.

Étape 12 Passez en revue et installez :

a) Passez en revue l'installation.
b) Cliquez sur **Previous** (Précédent) pour revenir en arrière et apporter des modifications.
c) Cliquez sur **Install This Configuration** (Installer cette configuration) pour continuer avec les informations que vous avez fournies.

What to do next

Thèmes connexes

- Prévention de la perte de données sécurisées, on page 67
- Interfaces réseau, on page 26
- Configuration des routages de trafic TCP/IP, on page 43
- Configuration de la redirection transparente, on page 46
- Gestion des alertes, on page 590
- Configuration d'un hôte de relais SMTP, on page 56

Contrôle de l'accès au Web à l'aide des groupes de répertoires dans le nuage

Vous pouvez utiliser Cisco Cloud Web Security pour contrôler l'accès Web en fonction des groupes de répertoires. Lorsque le trafic vers Cisco Cloud Web Security est acheminé par l'intermédiaire d'un Secure Web Appliance en mode Cloud Connector, Cisco Cloud Web Security doit recevoir les informations de groupe de répertoires avec les transactions de Cloud Connector pour pouvoir appliquer les politiques de nuage basées sur les groupes.

Before you begin

Ajoutez un domaine d'authentification à la configuration Secure Web Appliance.

Étape 1 Accédez à **Network** > **Cloud Connector** (Réseau > Cloud Connector).

Étape 2 Dans la zone **Cloud Policy Directory Groups** (Groupes d'annuaires de politiques de nuage), cliquez sur **Edit Groups** (Modifier les groupes).

Étape 3 Sélectionner les groupes d'utilisateurs et les groupes d'ordinateurs pour lesquels vous avez créé des politiques de nuage dans Cisco Cloud Web Security.

Étape 4 Cliquez sur **Add** (Ajouter).

Étape 5 Cliquez sur **Done** (Terminé) et validez vos modifications.

What to do next

Informations connexes

• Domaines d'authentification, on page 115

Contournement du serveur proxy dans le nuage

Les politiques de routage dans le nuage vous permettent d'acheminer le trafic Web vers les proxys Cisco Cloud Web Security ou directement vers Internet sur la base des caractéristiques suivantes :

- **Identification Profile** (Profil d'identification)
- Proxy Port (Port du serveur proxy)
- Subnet (Sous-réseau)
- URL Category (Catégorie URL)
- User Agent (Agent d'utilisateur)

Le processus de création de politiques de routage du nuage en mode Cloud Connector est identique au processus de création de politiques de routage en mode standard.

Thèmes connexes

• Création d'une politique , on page 253

Prise en charge partielle de FTP et HTTPS en mode Cloud Connector

Secure Web Appliance en mode Cloud Connector ne prend pas entièrement en charge FTP ou HTTPS.

FTP

FTP n'est pas pris en charge par Cloud Connector. AsyncOS abandonne le trafic FTP natif lorsque l'appliance est configurée pour Cloud Connector.

FTP sur HTTP est pris en charge en mode Cloud Connector.

HTTPS

Cloud Connector ne prend pas en charge le déchiffrement. Il transmet le trafic HTTPS sans déchiffrer.

Comme Cloud Connector ne prend pas en charge le déchiffrement, AsyncOS n'a généralement pas accès aux informations dans les en-têtes clients du trafic HTTPS. Par conséquent, AsyncOS ne peut généralement pas appliquer les politiques de routage qui reposent sur les informations contenues dans les en-têtes chiffrés. C'est toujours le cas pour les transactions HTTPS transparentes. Par exemple, pour les transactions HTTPS transparentes, AsyncOS n'a pas accès au numéro de port dans l'en-tête du client HTTPS et, par conséquent, il ne peut pas correspondre à une politique de routage basée sur le numéro de port. Dans ce cas, AsyncOS utilise la politique de routage par défaut.

Il y a deux exceptions pour les transactions HTTPS explicites. AsyncOS a accès aux informations suivantes pour les transactions HTTPS explicites :

- URL
- Numéro du port de destination

Pour les transactions HTTPS explicites, il est possible de mettre en correspondance une politique de routage basée sur l'URL ou le numéro de port.

Prévention de la perte de données sécurisées

Vous pouvez intégrer Cloud Connector à des serveurs externes de protection contre la perte de données en sélectionnant **Network** > **External DLP Servers** (Réseau > Serveur DLP externes).

Thèmes connexes

- Prévenir la perte de données sensibles, on page 357

Affichage des noms d'utilisateurs et de groupes et des adresses IP

Pour afficher les noms de groupes, les noms d'utilisateur et les adresses IP configurés, accédez à la page whoami.scansafe.net.

Abonnement aux journaux Cloud Connector

Les journaux Cloud Connector fournissent des informations utiles pour résoudre les problèmes rencontrés par Cloud Connector, par exemple, les utilisateurs et les groupes authentifiés, l'en-tête en nuage et la clé d'autorisation.

Étape 1 Accédez à **System Administration** > **Log Subscriptions** (Administration système > Abonnement aux journaux).

Étape 2 Sélectionnez **Cloud Connector Logs** (Journaux Cloud Connector) dans le menu **Log Type** (Type de journal).

Étape 3 Tapez un nom dans le champ **Log Name** (Nom du journal).

Étape 4 Définissez le niveau de journalisation.

Étape 5 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Superviser l'activité du système au moyen de journaux, on page 483

Profils d'identification et authentification avec Cloud Web Security Connector

Cloud Web Security Connector prend en charge l'authentification de base et NTLM. Vous pouvez également contourner l'authentification pour certaines destinations.

En mode Cloud Connector, à l'aide d'un domaine Active Directory, vous pouvez identifier les demandes de transaction comme provenant d'ordinateurs spécifiques. Le service d'ID d'ordinateur n'est pas disponible en mode standard.

À deux exceptions près, l'authentification fonctionne de la même manière dans Secure Web Appliance, que ce soit dans la configuration standard ou dans la configuration Cloud Connector. Exceptions :

- Le service d'ID d'ordinateur n'est pas disponible en mode standard.
- AsyncOS ne prend pas en charge Kerberos lorsque l'appliance est configurée en mode Cloud Connector.

Note Les profils d'identification basés sur l'agent utilisateur ou l'URL de destination ne sont pas pris en charge pour le trafic HTTPS.

Thèmes connexes

- Identification des ordinateurs pour l'application des politiques, on page 68
- Accès invité pour les utilisateurs non authentifiés, on page 69
- Classifier les utilisateurs finaux pour l'application des politiques, on page 151
- Survol de l'acquisition des informations d'authentification de l'utilisateur final, on page 101

Identification des ordinateurs pour l'application des politiques

En activant le service d'ID d'ordinateur, AsyncOS peut appliquer des politiques basées sur l'ordinateur qui a effectué la demande de transaction plutôt que sur l'utilisateur authentifié, l'adresse IP ou un autre identifiant. AsyncOS utilise NetBIOS pour acquérir l'ID de l'ordinateur.

Note Sachez que le service d'identité de l'ordinateur n'est disponible que par le biais des domaines Active Directory. Si aucun domaine Active Directory n'est configuré, ce service est désactivé.

Étape 1 Sélectionnez **Network > Machine ID Service** (Réseau > Service d'ID d'ordinateur).

Étape 2 Cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Étape 3 Configurez les paramètres d'identification de l'ordinateur :

Paramètres	Description
Enable NetBIOS for Machine Identification (Activer NetBIOS pour l'identification de l'ordinateur)	Sélectionnez cette option pour activer le service d'identification de l'ordinateur.
Realm (Domaine)	Le domaine Active Directory à utiliser pour identifier l'ordinateur qui lance la demande de transaction.
Failure Handling (Gestion des échecs)	Si AsyncOS ne peut pas identifier l'ordinateur, doit-il abandonner la transaction ou continuer la mise en correspondance de politiques?

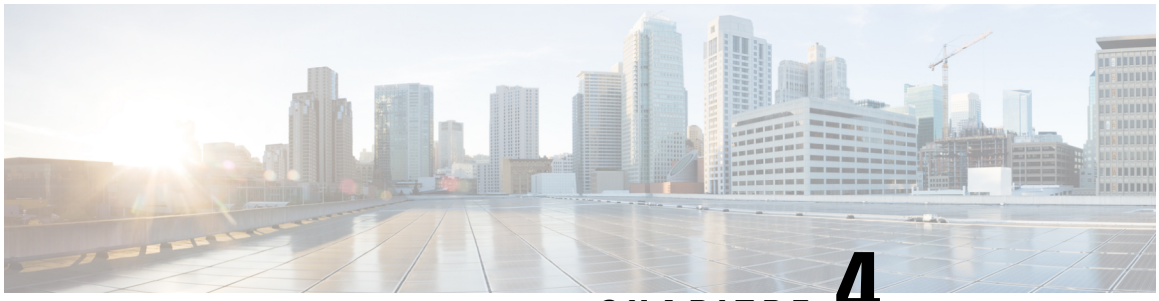
Étape 4 Envoyez et validez vos modifications.

Accès invité pour les utilisateurs non authentifiés

Si Secure Web Appliance est configuré pour fournir un accès invité aux utilisateurs non authentifiés, en mode Cloud Connector, AsyncOS affecte les utilisateurs invités au groupe __GUEST_GROUP__ et envoie ces informations à Cisco Cloud Web Security. Utilisez des identités pour fournir un accès invité aux utilisateurs non authentifiés. Utilisez les politiques Cisco Cloud Web Security pour contrôler ces utilisateurs invités.

Thèmes connexes

- Octroi d'un accès invité après échec de l'authentification, on page 144



CHAPITRE 4

Interception des demandes Web

Cette rubrique contient les sections suivantes :

Survol de l'interception des demandes Web

Secure Web Appliance intercepte les demandes qui lui sont transmises par les clients ou d'autres appareils sur le réseau.

L'appliance fonctionne de pair avec d'autres appareils réseau pour intercepter le trafic. Il peut s'agir de commutateurs simples, d'appareils de redirection transparents, de dérivateurs réseau et d'autres serveurs proxy ou Secure Web Appliance.

Tâches d'interception des demandes Web

Étapes	Tâche	Liens vers des rubriques et des procédures connexes
Étape 1	Passez en revue les bonnes pratiques.	• Bonnes pratiques pour l'interception des demandes Web, on page 72

Étapes	Tâche	Liens vers des rubriques et des procédures connexes
Étape 2	(Facultatif) Effectuez les tâches de mise en réseau suivantes : • Connectez-vous et configurez les proxy en amont. • Configurez les ports d'interface réseau : • Configurez les périphériques de redirection transparents. • Configurez les voies de routage TCP/IP. • Configurez les réseaux VLAN.	• Serveurs proxy en amont, on page 25 • Interfaces réseau, on page 26 • Configuration de la redirection transparente, on page 46 • Configuration des routages de trafic TCP/IP, on page 43 • Augmentation de la capacité de l'interface à l'aide de VLAN, on page 53
Étape 3	(Facultatif) Effectuez les tâches relatives au proxy Web : • Configurez le proxy Web pour qu'il fonctionne en mode transfert ou transparent. • Déterminez si des services supplémentaires sont nécessaires pour les types de protocoles que vous souhaitez intercepter • Configurez l'usurpation d'adresses IP. • Gérez le cache du proxy Web. • Utilisez des en-têtes de demande Web personnalisés. • Contournez le proxy pour certaines demandes.	• Options de proxy Web pour l'interception des demandes Web, on page 73 • Configuration des paramètres du proxy Web, on page 73 • Options de proxy Web pour l'interception des demandes Web, on page 73 • Cache du proxy Web, on page 77 • Usurpation d'adresses IP de proxy Web, on page 79 • Contournement du proxy Web, on page 82
Étape 4	Effectuez les tâches du client : • Décidez comment les clients doivent rediriger les demandes vers le proxy Web. • Configurez les clients et les ressources du client.	• Options du client pour la redirection des demandes Web, on page 88 • Utilisation de fichiers PAC avec les applications clientes, on page 89
Étape 5	(Facultatif) Activez et configurez le proxy FTP.	• Services de proxy FTP, on page 92

Bonnes pratiques pour l'interception des demandes Web

- Activez uniquement les services proxy dont vous avez besoin.
- Utilisez la même méthode de transfert et de retour (L2 ou GRE) pour tous les services WCCP définis à la section Secure Web Appliance. Cela permet le fonctionnement cohérent de la liste de contournement de proxy.

- Veillez à ce que les utilisateurs ne puissent pas accéder aux fichiers PAC depuis l'extérieur du réseau de l'entreprise. Cela permet à vos télétravailleurs d'utiliser le proxy Web lorsqu'ils se trouvent sur le réseau de l'entreprise et de se connecter directement aux serveurs Web à d'autres moments.
- Autorisez un proxy Web à accepter les en-têtes X-Forwarded-For de proxys en aval ou d'équilibreurs de charge dignes de confiance uniquement.
- Laissez le proxy Web dans le mode transparent par défaut, même si vous utilisez uniquement le transfert explicite au départ. Le mode transparent accepte également les demandes explicitement transférées.

Options de proxy Web pour l'interception des demandes Web

À lui seul, le proxy Web peut intercepter les demandes Web qui utilisent HTTP (y compris FTP sur HTTP) et HTTPS. Des modules de proxy supplémentaires sont disponibles pour améliorer la gestion des protocoles :

- **Proxy FTP.** Le proxy FTP permet l'interception du trafic FTP natif (plutôt que simplement du trafic FTP qui a été codé dans HTTP).
- **Proxy HTTPS.** Le proxy HTTPS prend en charge le déchiffrement du trafic HTTPS et permet au proxy Web de transmettre les requêtes HTTPS non chiffrées aux politiques pour l'analyse de contenu.

Note En mode transparent, le proxy Web abandonne toutes les requêtes HTTPS redirigées de manière transparente si le proxy HTTPS n'est pas activé. Aucune entrée de journal n'est créée pour les demandes HTTPS abandonnées redirigées de manière transparente.

- **Proxy SOCKS.** Le proxy SOCKS permet l'interception du trafic SOCKS.

Chacun de ces proxy supplémentaires nécessite le proxy Web pour fonctionner. Vous ne pouvez pas les activer si vous désactivez le proxy Web.

Note Le proxy Web est activé par défaut. Tous les autres proxys sont désactivés par défaut.

Thèmes connexes

- Services de proxy FTP, on page 92
- Services proxy SOCKS, on page 94

Configuration des paramètres du proxy Web

Before you begin

Activez le proxy Web.

Étape 1 Choisissez **Security Services** > **Web Proxy** (Services de sécurité > Proxy Web).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Configurez les paramètres de base du proxy Web au besoin.

Propriété	Description
HTTP Ports to Proxy (Ports HTTP vers proxy)	Ports sur lesquels le proxy Web écoute les connexions HTTP
Caching (Mise en mémoire cache)	Indique s'il faut activer ou désactiver la mise en cache du proxy Web. Le proxy Web met en cache les données pour augmenter les performances.
Proxy Mode (Mode proxy)	• **Transparent** (recommandé) : permet au proxy Web de nommer la cible Internet. Le proxy Web peut intercepter les demandes Web transparentes et explicitement transférées dans ce mode. • **Forward** (Transférer) : permet au navigateur client de nommer la cible Internet. Nécessite la configuration individuelle de chaque navigateur Web pour utiliser le proxy Web. Le proxy Web ne peut intercepter que les demandes Web explicitement transférées dans ce mode.
IP Spoofing Connection Type (Type de connexion d'usurpation d'adresses IP)	Si vous avez sélectionné le mode proxy **Transparent**, choisissez l'un des types de connexion d'usurpation d'adresses IP : • **For Transparent Connections Only** (Pour les connexions transparentes uniquement) : pour configurer l'usurpation d'adresses IP pour les connexions transparentes uniquement. • **For All Connections** (Pour toutes les connexions) : pour configurer l'usurpation d'adresses IP pour les connexions transparentes et explicites. Si vous avez sélectionné le mode proxy **Forward** (Transfert), le type de connexion d'usurpation d'adresses IP est toujours explicite. **Note** Le type de connexion d'usurpation d'adresses IP que vous choisissez est applicable à tous les protocoles : FTP natif, HTTP et HTTPS. Pour ajouter des profils d'usurpation d'adresses IP dans les politiques de routage, consultez Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage, on page 258

Étape 4 Renseignez les paramètres de proxy Web avancés comme requis.

Propriété	Description
Persistent Connection Timeout (Expiration de la connexion persistante)	Durée maximale en secondes pendant laquelle le proxy Web maintient ouverte une connexion avec un client ou un serveur après qu'une transaction est terminée et qu'aucune autre activité n'est détectée. • **Client side** (Côté client). Valeur du délai d'expiration pour les connexions aux clients. • **Server side** (Côté serveur). Valeur du délai d'expiration pour les connexions aux serveurs. Si vous augmentez ces valeurs, les connexions resteront ouvertes plus longtemps et réduiront le surdébit utilisé pour ouvrir et fermer des connexions à plusieurs reprises. Cependant, vous réduisez également la capacité du proxy Web à ouvrir de nouvelles connexions si le nombre maximal de connexions persistantes simultanées a été atteint. Après avoir établi une connexion et effectué une liaison SSL, si les demandes du client ne sont pas envoyées au proxy, ce dernier attend l'expiration du délai de connexion persistante, puis met fin à la connexion avec le client. Cisco recommande de conserver les valeurs par défaut.
In-Use Connection Timeout (Délai d'expiration de la connexion en cours d'utilisation)	Durée maximale en secondes pendant laquelle le proxy Web attend davantage de données d'un client ou d'un serveur inactif lorsque la transaction en cours n'est pas encore terminée. • **Client side** (Côté client). Valeur du délai d'expiration pour les connexions aux clients. • **Server side** (Côté serveur). Valeur du délai d'expiration pour les connexions aux serveurs.
Simultaneous Persistent Connections (Server Maximum Number) [Connexions persistantes simultanées (nombre maximum de serveurs)]	Le nombre maximal de connexions (prises) que le proxy Web maintient ouvertes avec les serveurs.
Maximum Connections Per Client (Nombre maximal de connexions par client)	Limite le nombre de connexions simultanées initiées par le client à une valeur configurée. Lorsque le nombre de connexions dépasse la limite configurée, les connexions sont abandonnées et une alerte est envoyée à l'administrateur. **Note** Par défaut, le nombre maximal de connexions par client est désactivé. Pour configurer la limite, cochez la case **Maximum Connections Per Client** (Nombre maximal de connexions par client) et procédez comme suit : • **Connexions** (Connections) : saisissez le nombre de connexions simultanées admissibles. • **Exempted Downstream Proxy or Load Balancer** (Équilibre de charge ou proxy en aval dispensé) : saisissez l'adresse IP du proxy en aval, de l'équilibreur de charge ou de toute autre adresse IP client (vous ne pouvez pas configurer les sous-réseaux ou les noms d'hôte). Le proxy Web n'applique pas les restrictions des connexions simultanées aux adresses IP incluses dans cette liste de dispenses.

Propriété	Description
Generate Headers (Générer des en-têtes)	Générez et ajoutez des en-têtes qui codent les informations concernant la demande. • Les en-têtes **X-Forwarded-For** codent l'adresse IP du client d'où provient une demande HTTP. **Note** • Pour activer ou désactiver le transfert d'en-tête, utilisez l'option Miscellaneous (Divers) de la commande de l'interface de ligne de commande `advancedproxyconfig`, Do you want to pass HTTP X-Forwarded-For headers? (Voulez-vous transférer les en-têtes HTTP X-Forwarded-For?) • L'utilisation d'un proxy de transfert en amont explicite pour gérer l'authentification d'utilisateurs ou le contrôle d'accès avec authentification de proxy nécessite le transfert de ces en-têtes. • Pour les demandes HTTPS transparentes, l'appliance ne déchiffre pas l'en-tête XFF. Pour les demandes explicites, l'appliance utilise l'en-tête XFF reçu dans la demande CONNECT et ne déchiffre pas XFF à l'intérieur du tunnel SSL, de sorte que l'identification des adresses IP des clients à l'aide de X-Forwarded-For n'est pas applicable aux demandes HTTPS transparentes. • Les en-tête **Request Side VIA** (VIA côté demande) encodent les proxys par lesquels passe la demande pendant sa transmission du client au serveur. • Les en-têtes **Response Side VIA** (VIA côté réponse) encodent les proxys par lesquels passe la demande pendant sa transmission du serveur au client.
Use Received Headers (Utiliser les en-têtes reçus)	Permet à un proxy Web déployé en tant que proxy en amont d'identifier les clients à l'aide des en-têtes X-Forwarded-For envoyés par les proxys en aval. Le proxy Web n'acceptera pas l'adresse IP dans un en-tête X-Forwarded-For provenant d'une source qui n'est pas incluse dans cette liste. Si cette option est activée, elle nécessite l'adresse IP d'un proxy en aval ou d'un équilibreur de charge (vous ne pouvez pas saisir de sous-réseaux ni de noms d'hôte).
Range Request Forwarding (Transfert de demande de plage)	Cochez la case **Enable Range Request Forwarding** (Activer le transfert des demandes de plage) pour activer ou désactiver le transfert des demandes de plage. Voir Gestion de l'accès aux applications Web, on page 347 pour plus d'informations.

Étape 5 Envoyez et validez vos modifications.

What to do next

- Cache du proxy Web, on page 77
- Configuration de la redirection transparente, on page 46

Cache du proxy Web

Le proxy Web met en cache les données pour augmenter les performances. AsyncOS comprend des modes de mise en cache définis qui vont de sécurisé à dynamique, et permet également une mise en cache personnalisée. Vous pouvez également exclure des URL spécifiques de la mise en cache en les supprimant du cache ou en configurant le cache de sorte qu'il les ignore.

Effacement du cache du proxy Web

Étape 1 Choisissez **Security Services** > **Web Proxy** (Services de sécurité > Proxy Web).

Étape 2 Cliquez sur **Clear Cache** (Effacer le cache) et confirmez votre action.

Suppression d'URL du cache du proxy Web

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `webcache > evict` pour accéder à la zone de mise en cache requise :

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

Étape 3 Entrez l'URL à supprimer du cache.

Note Si vous n'incluez pas de protocole dans l'URL, `http://` lui sera ajouté en préfixe (p. ex., `www.cisco.com` deviendra `http://www.cisco.com`)

Spécification des domaines ou des URL que le proxy Web ne met jamais en mémoire cache

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `webcache` -> `ignore` pour accéder aux sous-menu requis :

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

Étape 3 Entrez le type d'adresse que vous souhaitez gérer : `DOMAINS` ou `URLS`.

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

Étape 4 Entrez **add** (ajouter) pour ajouter de nouvelles entrées :

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

Étape 5 Entrez les domaines ou les URL, un par ligne; par exemple :

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

Vous pouvez inclure certains caractères d'expression régulière (regex) lorsque vous spécifiez un domaine ou des URL. Avec l'option `DOMAINS`, vous pouvez utiliser un point pour dispenser un domaine entier et ses sous-domaines de la mise en cache. Par exemple, vous pouvez saisir `.google.com` plutôt que simplement `google.com` pour dispenser www.google.com, docs.google.com, etc.

Avec l'option `URLS`, vous pouvez utiliser la suite complète des caractères d'expression régulière. Consultez Expressions régulières, on page 224 pour plus d'informations sur l'utilisation des expressions régulières.

Étape 6 Lorsque vous avez terminé de saisir les valeurs, appuyez sur Entrée jusqu'à revenir à l'interface de ligne de commande principale.

Étape 7 Validez vos modifications.

Choix du mode de mise en mémoire cache du proxy Web

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `advancedproxyconfig -> caching` pour accéder aux sous-menus requis :

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

```
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

Étape 3 Saisissez le numéro correspondant aux paramètres de cache du proxy Web dont vous avez besoin :

Entrée de gamme	Mode	Description
1	Demandes	La mise en mémoire cache la plus faible et le plus grand respect de la RFC 2616 par rapport aux autres modes.
2	Optimisé	Mise en mémoire cache modérée et respect modérée de la RFC 2616. Par rapport au mode sans échec, en mode optimisé, le proxy Web met en mémoire cache les objets si aucune heure de mise en cache n'est spécifiée quand un en-tête Last-Modified est présent. Le proxy Web met en cache les réponses négatives.
3	Dynamique	La mise en cache la plus importante et le respect de la RFC 2616 le plus faible. Par rapport au mode optimisé, le mode dynamique met en cache le contenu authentifié, les incompatibilités d'ETag et le contenu sans en-tête Last-Modified. Le proxy Web ignore le paramètre no-cache.
4	Mode personnalisé	Configurez chaque paramètre individuellement.

Étape 4 Si vous avez choisi l'option 4 (mode personnalisé), saisissez des valeurs (ou conservez les valeurs par défaut) pour chacun des paramètres personnalisés.

Étape 5 Appuyez sur **Enter** (Entrée) jusqu'à ce que vous reveniez à l'interface de commande principale.

Étape 6 Validez vos modifications.

What to do next

Thèmes connexes

- Cache du proxy Web, on page 77.

Usurpation d'adresses IP de proxy Web

Lorsque le proxy Web transfère une demande, il modifie l'adresse IP de la source de la demande pour qu'elle corresponde à la sienne par défaut. Cela augmente la sécurité, mais vous pouvez modifier ce comportement en mettant en œuvre l'usurpation d'adresses IP, de sorte que les demandes semblent provenir de l'adresse IP du client ou de toute autre adresse IP personnalisée routable plutôt que de Secure Web Appliance. Vous pouvez configurer l'usurpation d'adresses IP du proxy Web en créant des profils d'usurpation d'adresses IP pour les adresses IP personnalisées et en les ajoutant aux politiques de routage.

L'usurpation d'adresses IP fonctionne pour un trafic transparent et explicitement transféré. Lorsque le proxy Web est déployé en mode transparent, vous pouvez configurer le type de connexion d'usurpation d'adresses

IP pour les connexions redirigées de manière transparente uniquement ou pour toutes les connexions (redirigées transparentes et explicitement transférées). Si les connexions explicitement transférées utilisent l'usurpation d'adresses IP, vous devez vous assurer que vous disposez des périphériques réseau appropriés pour acheminer les paquets de retour vers Secure Web Appliance.

Lorsque l'usurpation d'identités IP est activée et que l'appliance est connectée à un routeur WCCP, vous devez configurer deux services WCCP : un basé sur les ports source et un basé sur les ports de destination.

Les profils d'usurpation d'adresses IP sont limités lorsque le trafic HTTPS est redirigé de manière transparente. Consultez Accès aux sites HTTPS à l'aide de politiques de routage avec critères de catégorie d'URL, on page 642.

Thèmes connexes

- Création de profils d'usurpation d'adresses IP, on page 80
- Configuration des paramètres du proxy Web, on page 73
- Configuration des services WCCP, on page 47

Création de profils d'usurpation d'adresses IP

Before you begin

Assurez-vous d'avoir sélectionné le mode proxy et le type de connexion d'usurpation d'adresses IP dans les paramètres de proxy Web. Pour en savoir plus, consultez Configuration des paramètres du proxy Web, on page 73.

Étape 1 Choisissez **Web Security Manager** > **IP Spoofing Profiles** (Web Security Manager > Profils d'usurpation d'adresses IP).

Étape 2 Cliquez sur **Add Profile** (Ajouter un profil).

Étape 3 Entrez un nom pour le profil d'usurpation d'adresses IP.

Étape 4 Entrez l'adresse IP que vous souhaitez attribuer au nom de profil d'usurpation d'identité.

Étape 5 Envoyez et validez vos modifications.

What to do next

Ajouter le profil d'usurpation d'adresses IP à une politique de routage. Pour en savoir plus, consultez Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage, on page 258.

Related Topics

Modification des profils d'usurpation d'adresses IP, à la page 80
Suppression des profils d'usurpation d'adresses IP, à la page 81

Modification des profils d'usurpation d'adresses IP

Note Une fois que vous avez mis à jour un profil d'usurpation d'adresses IP, il sera mis à jour dans toutes les politiques de routage associées à ce profil.

Étape 1 Choisissez **Web Security Manager** > **IP Spoofing Profiles** (Web Security Manager > Profils d'usurpation d'adresses IP).

Étape 2 Cliquez sur le lien du nom du profil d'usurpation IP que vous souhaitez modifier.

Étape 3 Modifiez les détails du profil.

Étape 4 Envoyez et validez vos modifications.

Suppression des profils d'usurpation d'adresses IP

Étape 1 Choisissez **Web Security Manager** > **IP Spoofing Profiles** (Web Security Manager > Profils d'usurpation d'adresses IP).

Étape 2 Cliquez sur l'icône de corbeille correspondant au profil d'usurpation d'adresses IP que vous souhaitez supprimer.

Note L'appliance affiche un avertissement si le profil d'usurpation d'adresses IP que vous supprimez est affecté à une ou plusieurs politiques de routage. Dans ce cas, sélectionnez un autre profil d'usurpation d'adresses IP à affecter à toutes les politiques de routage concernées.

Étape 3 Envoyez et validez vos modifications.

En-têtes personnalisés de proxy Web

Vous pouvez ajouter des en-têtes personnalisés à des transactions sortantes spécifiques pour demander un traitement spécial aux serveurs de destination. Par exemple, si vous avez une relation avec YouTube pour les écoles, vous pouvez utiliser un en-tête personnalisé pour identifier les demandes de transaction adressées à YouTube.com comme provenant de votre réseau et comme nécessitant un traitement spécial.

Ajout d'en-têtes personnalisés aux demandes Web

Étape 1 Accédez à l'interface de ligne de commande.

Étape 2 Utilisez les commandes `advancedproxyconfig -> customheaders` pour accéder aux sous-menus requis :

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
```

```
- EDIT - Edit entries
[]>
```

Étape 3 Utilisez la sous-commande requise comme suit :

Option	Description
`Delete` (Supprimer)	Supprime l'en-tête personnalisé que vous identifiez. Identifiez l'en-tête à supprimer en utilisant le numéro associé à l'en-tête dans la liste renvoyée par la commande.
`New` (Nouveau)	Crée l'en-tête que vous fournissez à utiliser avec le domaine ou les domaines que vous spécifiez. Exemple d'en-tête : X-YouTube-Edu-Filter : ABCD1234567890abcdef (Dans ce cas, la valeur est une clé unique fournie par YouTube.) Exemple de domaine : youtube.com
`Edit` (Modifier)	Remplace un en-tête existant par un que vous spécifiez. Identifiez l'en-tête à supprimer en utilisant le numéro associé à l'en-tête dans la liste renvoyée par la commande.

Étape 4 Appuyez sur **Enter** (Entrée) jusqu'à ce que vous reveniez à l'interface de commande principale.

Étape 5 Validez vos modifications.

Contournement du proxy Web

Contournement du proxy Web pour les demandes Web

Vous pouvez configurer Secure Web Appliance de sorte que les demandes transparentes de clients particuliers ou vers des destinations particulières contournent le proxy Web.

En contournant le proxy Web, vous pouvez :

- Éviter les interférences avec les protocoles non conformes (ou propriétaires) qui utilisent des ports HTTP mais ne fonctionnent pas correctement lorsqu'ils se connectent à un serveur proxy.
- Veiller à ce que le trafic provenant d'une machine particulière du réseau, comme une machine de test de programmes malveillants, contourne le proxy Web et toutes ses protections de sécurité intégrées.

Le contournement ne fonctionne que pour les demandes qui sont redirigées de manière transparente vers le proxy Web. Le proxy Web traite toutes les demandes que les clients lui transmettent explicitement, que le proxy soit en mode transparent ou renvoi.

Configuration du contournement du proxy Web pour les demandes Web

Étape 1 Choisissez **Web Security Manager > Bypass Settings** (Web Security Manager > Contourner les paramètres).

Étape 2 Cliquez sur **Edit Bypass Settings** (Modifier les paramètres de contournement).

Étape 3 Entrez les adresses pour lesquelles vous souhaitez contourner le proxy Web.

Note Lorsque vous configurez /0 comme masque de sous-réseau pour une adresse IP dans la liste de contournement, l'appliance contourne tout le trafic Web. Dans ce cas, l'appliance interprète la configuration comme 0.0.0.0/0.

Étape 4 Choisissez les catégories d'URL personnalisées que vous souhaitez ajouter à la liste de contournement de proxy.

Note Vous ne pouvez pas définir le contournement de proxy Web pour les expressions régulières.

Note Une fois que vous avez ajouté les catégories d'URL personnalisées à la liste de contournement de proxy, toutes les adresses IP et les noms de domaine des catégories d'URL personnalisées sont contournés pour la source et la destination.

Étape 5 Envoyez et validez vos modifications.

Configuration du contournement du proxy Web pour les applications

Étape 1 Choisissez **Web Security Manager > Bypass Settings** (Web Security Manager > Contourner les paramètres).

Étape 2 Cliquez sur **Edit Application Bypass Settings** (Modifier les paramètres de contournement d'application).

Étape 3 Sélectionnez les applications pour lesquelles vous souhaitez contourner l'analyse.

Étape 4 Envoyez et validez vos modifications.

Note Les paramètres de contournement de Webex ne s'appliquent qu'au trafic HTTPS. Cependant, pour le trafic HTTP, les applications peuvent être bloquées par les politiques d'accès.

En-têtes personnalisés du proxy Web par politique

Vous pouvez configurer des profils d'en-tête personnalisés pour les requêtes HTTP et créer plusieurs en-têtes dans un profil de réécriture d'en-tête. Chaque profil peut comprendre un maximum de 12 en-têtes. Vous pouvez également modifier ou supprimer les profils d'en-tête existants. Vous pouvez ajouter le profil de réécriture d'en-tête à une politique d'accès existante pour inclure les en-têtes dans toutes les transactions auxquelles la politique d'accès particulière est appliquée.

La fonction de profil de réécriture d'en-tête permet à l'appliance de transmettre les informations sur l'utilisateur et le groupe à un autre périphérique en amont une fois l'authentification réussie. Le proxy en amont considère l'utilisateur comme authentifié, contourne l'authentification supplémentaire et fournit un accès à l'utilisateur en fonction des politiques d'accès définies.

- Création de profils de réécriture d'en-têtes pour les demandes Web HTTP, à la page 84
- Modification des formats de nom d'utilisateur et d'en-tête de groupe , à la page 85 (facultatif)

• Ajout de profils d'en-tête à la politique d'accès, à la page 86

Il est recommandé de ne pas créer d'en-têtes de proxy Web personnalisés à l'aide de la commande d'interface de ligne de commande `advancedproxyconfig -> customheader` à partir d'AsynOS version 14.0.

Création de profils de réécriture d'en-têtes pour les demandes Web HTTP

Étape 1 Choisissez **Web Security Manager** -> **HTTP Rewrite Profiles** (Web Security Manager > Profils de réécriture http).

Étape 2 Cliquez sur **Add Profile** (Ajouter un profil).

Étape 3 Attribuez un nom unique au profil de réécriture d'en-tête que vous souhaitez créer.

Étape 4 Dans la zone **Headers** (En-têtes), saisissez les informations suivantes :

Remarque Vous pouvez saisir une valeur d'en-tête vide ou nulle dans Header Rewrite Profiles (Profils de réécriture d'en-tête). Lorsque vous enregistrez et validez l'en-tête ne contenant aucune valeur ou contenant une valeur nulle, l'en-tête n'est pas inclus dans les demandes sortantes. Par exemple, si vous souhaitez masquer l'en-tête `Via` sur le serveur sortant, ajoutez le nom d'en-tête `Via` aux profils de réécriture HTTP avec la valeur "".

- **Header Name** (Nom d'en-tête) : Saisissez le nom d'en-tête que vous souhaitez ajouter aux demandes HTTP. Exemple : X-Client-IP, X-Authenticated-User, X-Authenticated-Groups, etc.
- **Header Value** (Valeur d'en-tête) : Saisissez la valeur à inclure dans l'en-tête de demande correspondant au nom d'en-tête. Ajouter aux variables d'en-tête le préfixe suivant :
  - `$ReqMeta`— Pour récupérer les variables d'en-tête HTTP standard telles que l'adresse IP du client, l'utilisateur, le groupe, etc. Par exemple, pour inclure le nom d'utilisateur dans l'en-tête de la demande, le format est `($ReqMeta[X-Authenticated-User])`
  - `$ReqHeader` : Pour utiliser les valeurs des en-têtes HTTP standard ou les valeurs d'autres en-têtes définis sous le même profil de réécriture d'en-tête.

    Par exemple :

    ```
    En-tête 1 :32

    En-tête 2 : 44-($ReqHeader[Header1])-46
    ```

    La valeur de l'`en-tête 2` est `44-32-46`
- **Text Format** (Format de texte) : Choisissez le format de texte pour l'encodage. Les options disponibles sont ASCII et UTF-8.
- **Binary Encoding** (Codage binaire) : Choisissez si vous souhaitez ou non l'encodage binaire (Base64) pour les en-têtes de demande.

Remarque Selon le type de serveur, l'appliance affiche un message d'erreur si la taille du champ d'en-tête de la demande envoyée dépasse la limite maximale du serveur. Par exemple, différents types de serveurs prennent en charge différentes longueurs d'en-tête :

- Apache 2.0, 2.2 : 8k
- Nginx : 4k - 8k
- IIS (varie selon la version) : 8K - 16K
- Tomcat : (varie selon la version) 8K

Si l'identification de l'utilisateur utilise le service ISE, les paramètres globaux des en-têtes X-Authentication, c'est-à-dire X-Authenticated-User et X-Authenticated-Groups, n'appliquent pas de domaine et de mécanisme d'authentification comme préfixe.

Vous pouvez saisir UTF+8 comme valeur `($ReqMeta[HTTP_header])` même si vous sélectionnez le format de texte ASCII. Les en-têtes suivants prennent actuellement en charge `($ReqMeta[HTTP_tête])` :

- X-Authenticated-User
- X-Authenticated-Groups
- X-Client-IP

Les en-têtes ne sont pas inclus dans les demandes sortantes si les valeurs des en-têtes sont nulles. Cela se produit lorsque vous :

- Activez l'authentification du proxy
- Définissez des groupes dans les critères d'appartenance pour la politique d'accès, la politique de déchiffrement ou la politique de routage.

Étape 5 Envoyez et validez vos modifications.

Modification des formats de nom d'utilisateur et d'en-tête de groupe

Étape 1 Choisissez **Web Security Manager** > **HTTP Rewrite Profiles** (Web Security Manager > Profils de réécriture HTTP).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Modifiez les formats.

Les formats autorisés sont les suivants :

- Nom d'utilisateur :`$authMechanism://$domainName/$userName, $authMechanism:\\$domainName\$userName, $domainName/$userName, $domainName\$userName, $userName`
- Groupe : `$authMechanism://$domainName/$groupName, $authMechanism:\\$domainName\$groupName, $domainName/$groupName, $domainName\$groupName, $groupName`

  Vous pouvez également modifier le séparateur, comme la virgule (,), les deux-points (:), le point-virgule (;), la barre oblique inverse (\), la barre verticale (|), etc.

Étape 4 Envoyez et validez vos modifications.

Ajout de profils d'en-tête à la politique d'accès

Avant de commencer

Configurez la politique d'accès. Consultez Création d'une politique , à la page 253.

Étape 1 Choisissez **Web Security Manager** >**Access Policies** (Web Security Manager > Politiques d'accès)

Étape 2 Dans la page Access Policies (Politiques d'accès), cliquez sur le lien HTTP Rewrite Profile (Profil de réécriture HTTP).

Vous pouvez également créer une nouvelle politique d'accès et y ajouter le profil de réécriture d'en-tête. Pour créer une stratégie d'accès, consultezCréation d'une politique , à la page 253

Étape 3 Sélectionnez le profil de réécriture d'en-tête que vous souhaitez ajouter à la stratégie. Après votre ajout, les en-têtes sont inclus dans la transaction HTTP à laquelle la politique d'accès particulière est appliquée.

Étape 4 Envoyez et validez vos modifications.

Vous pouvez supprimer un profil de réécriture d'en-tête lié à une politique d'accès. Avant de le supprimer, choisissez un autre profil. Le profil sélectionné sera automatiquement appliqué aux politiques d'accès.

Contrat d'utilisation du proxy Web

Vous pouvez configurer Secure Web Appliance pour informer les utilisateurs qu'il filtre et surveille leur activité Web. Pour ce faire, l'appliance affiche une page de confirmation destinée à l'utilisateur final la première fois qu'un utilisateur accède à un navigateur après un certain temps. Lorsque la page de confirmation de l'utilisateur final s'affiche, les utilisateurs doivent cliquer sur un lien pour accéder au site initialement demandé ou à tout autre site Web.

Thèmes connexes

- Aviser les utilisateurs finaux des actions du proxy, on page 371

Mappage de domaine

Vous pouvez configurer Secure Web Appliance de sorte que les demandes HTTPS transparentes provenant de clients particuliers ou vers des destinations particulières contournent le proxy HTTPS.

Vous pouvez utiliser l'intercommunication pour les applications qui nécessitent que le trafic passe par l'appliance, sans subir de modification, ou de vérification de certificat des serveurs de destination.

Carte de domaine pour des applications spécifiques

Avant de commencer

Assurez-vous d'avoir défini une politique d'identification pour les appareils qui nécessitent un trafic de transit vers des serveurs spécifiques. Consultez Classification des utilisateurs et logiciels clients, à la page 153 pour obtenir de plus amples renseignements. Plus précisément, vous devez :

- Choisissez **Exempt from authentication/identification** (Dispenser de l'authentification/identification).
- Indiquer les adresses auxquelles ce profil d'identification doit s'appliquer. Vous pouvez utiliser des adresses IP, des blocs d'CIDR et des sous-réseaux.

Étape 1 Activer le proxy HTTPS. Consultez Activation du proxy HTTPS, à la page 283 pour obtenir de plus amples renseignements.

Étape 2 Choisissez **Web Security Manager** > **Domain Map** (Web Security Manager > Carte des domaines).

a) Cliquez sur **Add Domain** (Ajouter un domaine).
b) Renseignez le champ **Domain Name** (Nom du domaine) ou indiquez le serveur de destination.
c) Choisissez l'ordre de priorité si des domaines existants sont spécifiés.
d) Entrez les adresses IP.
e) Cliquez sur **Submit** (Soumettre).

Étape 3 Choisissez **Web Security Manager** > **Custom and External URL Categories** (Web Security Manager > Catégories d'URL personnalisées et externes).

a) Cliquez sur **Add Catégorie** (Ajouter une catégorie).
b) Indiquez les renseignements suivants.

Paramètres	Description
Category Name (Nom de la catégorie)	Entrez un identifiant pour cette catégorie d'URL. Ce nom s'affiche lorsque vous configurez le filtrage d'URL pour les groupes de politiques.
List Order (Ordre de la liste)	Précisez l'ordre de cette catégorie dans la liste des catégories d'URL personnalisées. Entrez « 1 » pour la première catégorie d'URL de la liste. Le moteur de filtrage d'URL évalue une demande d'un client par rapport aux catégories d'URL personnalisées dans l'ordre spécifié.
Category Type (Type de catégorie)	Choisissez **Local Custom Category** (Catégorie personnalisée locale).
Advanced (Niveau avancé)	Vous pouvez saisir des expressions régulières dans cette section pour spécifier des ensembles d'adresses supplémentaires. Vous pouvez utiliser des expressions régulières pour spécifier plusieurs adresses qui correspondent aux schémas que vous saisissez. Consultez Expressions régulières, à la page 224 pour plus d'informations sur l'utilisation des expressions régulières.

c) Envoyez et validez les modifications.

Étape 4 Choisissez **Web Security Manager** > **Decryption Policies** (Web Security Manager > Politiques de déchiffrement).

a) Créez une nouvelle politique de déchiffrement.
b) Choisissez le profil d'identification que vous avez créé pour contourner le trafic HTTPS pour des applications spécifiques.
c) Dans le panneau **Advanced** (Avancé), cliquez sur le lien URL Categories (Catégories d'URL).
d) Dans la colonne **Add** (Ajouter), cliquez pour ajouter la catégorie d'URL personnalisée créée à l'étape 3.
e) Cliquez sur **Done** (Terminé).
f) Dans la page des politiques de déchiffrement, cliquez sur le lien **URL Filtering** (Filtrage URL).
g) Choisissez **Pass Through** (Intercommunication).
h) Envoyez et validez les modifications.

Vous pouvez utiliser le spécificateur de format **%(** pour afficher les informations du journal d'accès. Consultez Personnalisation des journaux d'accès, à la page 523 pour obtenir de plus amples renseignements.

Remarque

- La fonctionnalité de carte de domaine fonctionne en mode transparent HTTPS.
- Cette fonctionnalité ne fonctionne pas en mode explicite et pour le trafic HTTP.
- La catégorie personnalisée locale doit être configurée pour autoriser le trafic utilisant cette fonctionnalité.
- L'activation de cette fonctionnalité modifiera ou attribuera le nom du serveur selon le nom de serveur configuré dans la carte de domaine, même si les informations SNI sont disponibles.
- Cette fonctionnalité ne bloque pas le trafic en fonction du nom de domaine si ce trafic correspond à la mappe de domaine et si la catégorie personnalisée, la politique de déchiffrement et l'action de transmission directe correspondantes sont configurés.
- L'authentification ne fonctionne pas avec cette fonctionnalité d'intercommunication. L'authentification doit être déchiffrée, mais le trafic ne sera pas déchiffré dans ce cas.
- Le trafic UDP n'est pas surveillé. Vous devez configurer le trafic UDP pour ne pas arriver à Secure Web Appliance, mais plutôt passer directement par le pare-feu vers Internet pour des applications comme WhatsApp, Telegram, etc.
- WhatsApp, Telegram et Skype fonctionnent en mode transparent. Cependant, certaines applications comme WhatsApp ne fonctionnent pas en mode explicite en raison de restrictions appliquées à l'application.

Options du client pour la redirection des demandes Web

Si vous choisissez que les clients transfèrent explicitement les demandes au proxy Web, vous devez également décider comment configurer les clients pour le faire. Choisissez l'une des méthodes suivantes :

- **Configure Clients Using Explicit Settings** (Configurer les clients à l'aide de paramètres explicites). Configurez les clients avec le nom d'hôte et le numéro de port du proxy Web. Consultez la documentation de chaque client pour savoir comment procéder.

Note Le port du proxy Web utilise les numéros de port 80 et 3128 par défaut. Les clients peuvent utiliser l'un ou l'autre de ces ports.

- **Configure Clients Using a Proxy Auto-Config (PAC) File** [Configurer les clients à l'aide d'un fichier PAC (Proxy Auto-Config)] Les fichiers PAC fournissent aux clients des instructions sur la destination des demandes Web. Cette option vous permet de gérer de manière centralisée les modifications ultérieures apportées aux détails du proxy.

Si vous choisissez d'utiliser des fichiers PAC, vous devez également choisir l'emplacement des fichiers et la façon dont les clients les trouveront.

Thèmes connexes

- Utilisation de fichiers PAC avec les applications clientes, on page 89

Utilisation de fichiers PAC avec les applications clientes

Options de publication des fichiers de configuration automatique de proxy (PAC)

Vous devez publier les fichiers PAC là où les clients peuvent y accéder. Les emplacements valides sont les suivants :

- **Serveurs Web.**
- **Secure Web Appliance**. Vous pouvez placer les fichiers PAC sur un Secure Web Appliance, qui s'affiche pour les clients comme un navigateur Web. L'appliance propose également des options supplémentaires pour la gestion des fichiers PAC, notamment la possibilité de traiter les demandes qui utilisent des noms d'hôte, des ports et des noms de fichiers différents.
- **Ordinateurs locaux.** Vous pouvez placer le fichier PAC localement sur le disque dur d'un client. Cisco ne recommande pas cette solution comme solution générale, et elle n'est pas adaptée aux méthodes de détection automatique des fichiers PAC, mais elle peut être utile pour les tests.

Thèmes connexes

- Hébergement des fichiers PAC sur Secure Web Appliance, on page 90
- Spécification des fichiers PAC dans les applications clientes, on page 91

- Hébergement des fichiers PAC sur Secure Web Appliance, on page 90
- Spécification des fichiers PAC dans les applications clientes, on page 91

Options du client pour la recherche des fichiers de configuration automatique de proxy (PAC)

Si vous choisissez d'utiliser des fichiers PAC pour vos clients, vous devez également décider comment les clients trouveront les fichiers PAC. Vous avez le choix entre deux options :

- **Configure client with the PAC file location** (Configurer le client avec l'emplacement du fichier PAC). Configurez le client avec une URL qui pointe spécifiquement vers le fichier PAC.
- **Configure clients to detect the PAC file location automatically** (Configurez les clients pour détecter automatiquement l'emplacement du fichier PAC). Configurez les clients pour qu'ils trouvent automatiquement les fichiers PAC à l'aide du protocole WPAD avec DHCP ou DNS.

Détection automatique des fichiers PAC

WPAD est un protocole qui permet au navigateur de déterminer l'emplacement d'un fichier PAC à l'aide de DHCP et DNS.

- **Pour utiliser WPAD avec DHCP**, vous devez configurer l'option 252 sur les serveurs DHCP avec l'URL de l'emplacement du fichier PAC. Cependant, tous les navigateurs ne prennent pas en charge DHCP.
- **Pour utiliser WPAD avec DNS**, vous devez configurer un enregistrement DNS pour qu'il pointe vers le serveur hôte du fichier PAC.

Vous pouvez configurer l'une ou l'autre des options ou les deux. WPAD essaiera d'abord de trouver les fichiers PAC à l'aide de DHCP. S'il ne peut pas, il essayera le DNS.

Thèmes connexes

- Détection automatique du fichier PAC sur les clients, on page 92

Hébergement des fichiers PAC sur Secure Web Appliance

Étape 1 Choisissez **Security Services > PAC File Hosting** (Services de sécurité > Hébergement de fichiers PAC).

Étape 2 Cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Étape 3 (Facultatif) Renseignez les paramètres de base suivants :

Option	Description
PAC Server Ports (Ports du serveur PAC)	Ports que Secure Web Appliance utilisera pour écouter les demandes de fichier PAC.
PAC File Expiration (Expiration du fichier PAC)	Autorise le fichier PAC à expirer après un nombre spécifié de minutes dans la mémoire cache du navigateur.

Étape 4 Cliquez sur **Browse** (Parcourir) dans la section PAC Files (Fichiers PAC), puis sélectionnez un fichier PAC sur votre machine locale pour le charger dans Secure Web Appliance.

Note Si le fichier que vous sélectionnez s'appelle `default.pac`, vous n'avez pas à spécifier le nom du fichier lors de la configuration de son emplacement dans un navigateur. Secure Web Appliance recherche un fichier appelé `default.pac` si aucun nom n'est spécifié.

Étape 5 Cliquez sur **Upload** (Charger) pour charger le fichier PAC sélectionné à l'étape 4 dans Secure Web Appliance.

Étape 6 (Facultatif) Dans la section Hostnames for Serving PAC Files Directly (Noms d'hôte pour la diffusion directe des fichiers PAC), configurez les noms d'hôte et les noms de fichiers associés pour les demandes de fichiers PAC qui ne comprennent pas de numéro de port :

Option	Description
Hostname (Nom d'hôte)	Nom d'hôte que la demande de fichier PAC doit inclure si Secure Web Appliance doit répondre à la demande. Comme la demande ne comprend pas de numéro de port, elle sera traitée sur les ports HTTP du proxy Web (p. ex., le port 80) et doit pouvoir être considérée comme une demande de fichier PAC par la valeur de ce nom d'hôte.
Default PAC File for "Get/" Request through Proxy Port (Fichier PAC par défaut pour la demande « Get/ » par le port de proxy)	Nom du fichier PAC qui sera associé au nom d'hôte sur la même ligne. La demande au nom d'hôte renverra le fichier PAC spécifié ici. Seuls les fichiers PAC qui ont été chargés peuvent être sélectionnés.
Add Row (Ajouter une ligne)	Ajoute une autre ligne pour spécifier des noms d'hôte et des noms de fichiers PAC supplémentaires.

Étape 7 Envoyez et validez vos modifications.

Spécification des fichiers PAC dans les applications clientes

Configuration manuelle de l'emplacement d'un fichier PAC sur les clients

Étape 1 Créez et publiez un fichier PAC.

Étape 2 Entrez une URL dans la zone de configuration du fichier PAC de votre navigateur qui pointe vers l'emplacement du fichier PAC.

Les formats d'URL suivants sont valides si Secure Web Appliance héberge le fichier PAC :

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

où *WSAHostname* correspond à la valeur du **nom d'hôte** configurée lors de l'hébergement du fichier PAC sur un Secure Web Appliance. Sinon, le format de l'URL dépendra de l'emplacement de stockage et, dans certains cas, du client.

What to do next

- Hébergement des fichiers PAC sur Secure Web Appliance, on page 90

Détection automatique du fichier PAC sur les clients

Étape 1 Créez un fichier PAC appelé wpad.dat et publiez-le sur un serveur Web ou Secure Web Appliance (le fichier doit être placé dans le dossier racine d'un serveur Web si vous souhaitez utiliser WPAD avec DNS).

Étape 2 Configurez le serveur Web pour installer les fichiers .dat avec le type MIME suivant :

```
application/x-ns-proxy-autoconfig
```

Note Un Secure Web Appliance le fait automatiquement pour vous.

Étape 3 Pour prendre en charge la recherche DNS, créez un nom DNS commençant par « `wpad` » pouvant être résolu en interne (par exemple, `wpad.exemple.com`) et associez-le à l'adresse IP du serveur qui héberge le fichier `wpad.dat`.

Étape 4 Pour prendre en charge la recherche DHCP, configurez l'option 252 de votre serveur DHCP avec l'URL de l'emplacement du fichier wpad.dat (par exemple : « `http://wpad.exemple.com/wpad.dat` »). L'URL peut utiliser n'importe quelle adresse hôte valide, notamment une adresse IP, et ne nécessite pas d'entrée DNS particulière.

What to do next

- Utilisation de fichiers PAC avec les applications clientes, on page 89
- Hébergement des fichiers PAC sur Secure Web Appliance, on page 90
- WPAD ne fonctionne pas avec Firefox, on page 637

Services de proxy FTP

- Survol des services proxy FTP, on page 92
- Activation et configuration du proxy FTP, on page 93

Survol des services proxy FTP

Le proxy Web peut intercepter deux types de demandes FTP :

- **FTP natif.** Les demandes FTP natives sont générées par des clients FTP dédiés (ou par des navigateurs utilisant des clients FTP intégrés). Nécessite le proxy FTP.
- **FTP sur HTTP.** Les navigateurs encodent parfois les requêtes FTP dans des demandes HTTP, plutôt que d'utiliser le FTP natif. Ne nécessitent pas le proxy FTP.

Thèmes connexes

- Activation et configuration du proxy FTP, on page 93
- Configuration des messages de notification FTP, on page 382

Activation et configuration du proxy FTP

Note Pour configurer les paramètres de proxy qui s'appliquent aux connexions FTP sur HTTP, consultez Configuration des paramètres du proxy Web, on page 73.

Étape 1 Choisissez **Security Services** > **FTP Proxy** (Services de sécurité > Proxy FTP).

Étape 2 Cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres) (si la seule option disponible est **Edit Settings** (Modifier les paramètres), le proxy FTP est déjà activé).

Étape 3 (Facultatif) Configurez les paramètres de base du proxy FTP.

Propriété	Description
Proxy Listening Port (Port d'écoute proxy)	Port sur lequel le proxy FTP sera à l'écoute pour les connexions de contrôle FTP. Les clients doivent utiliser ce port lors de la configuration d'un proxy FTP (et non comme port de connexion aux serveurs FTP, qui utilisent normalement le port 21).
Caching (Mise en mémoire cache)	Si les connexions de données d'utilisateurs anonymes sont ou non mises en cache. **Note** Les données des utilisateurs non anonymes ne sont jamais mises en cache.
Server Side IP Spoofing (Usurpation d'adresses IP côté serveur)	Permet au proxy FTP d'imiter l'adresse IP du serveur FTP. Cette option prend en charge les clients FTP qui n'autorisent pas les transactions lorsque l'adresse IP est différente pour les connexions de contrôle et de données.
Client IP Spoofing (Usurpation d'adresses IP du client)	Permet au proxy FTP d'imiter l'adresse IP source du client FTP. Lorsque cette option est activée, les demandes FTP semblent émaner du client FTP plutôt que du proxy FTP.
Authentication Format (Format d'authentification)	Offre un choix de format d'authentification que le proxy FTP peut utiliser lors de la communication avec des clients FTP.
Passive Mode Data Port Range (Plage de ports de données en mode passif)	Plage de ports TCP que les clients FTP doivent utiliser pour établir une connexion de données avec le proxy FTP pour les connexions en mode passif.
Active Mode Data Port Range (Plage du port de données en mode actif)	Plage de ports TCP que les serveurs FTP devraient utiliser pour établir une connexion de données avec le proxy FTP pour les connexions en mode actif. Ce paramètre s'applique aux connexions FTP natives et FTP sur HTTP. L'augmentation de la plage de ports permet de traiter un plus grand nombre de demandes du même serveur FTP. En raison du délai TIME-WAIT de la session TCP (généralement quelques minutes), un port ne redevient pas disponible pour le *même* serveur FTP immédiatement après avoir été utilisé. Par conséquent, un serveur FTP donné ne peut pas se connecter au proxy FTP en mode actif plus de *n* fois dans un court laps de temps, *n* étant le nombre de ports indiqué dans ce champ.

Propriété	Description
Welcome Banner (Bannière de bienvenue)	La bannière de bienvenue qui s'affiche sur les clients FTP lors de la connexion. Choisissez parmi : • **FTP server message** (Message du serveur FTP). Le message sera fourni par le serveur FTP de destination. Cette option est uniquement disponible lorsque le proxy Web est configuré pour le mode transparent et s'applique uniquement aux connexions transparentes. • **Custom message** (Message personnalisé). Lorsque cette option est sélectionnée, ce message personnalisé s'affiche pour toutes les connexions FTP natives. Lorsqu'elle n'est pas sélectionnée, elle est toujours utilisée pour les connexions FTP natives de transfert explicite.

Étape 4 (Facultatif) Configurez les paramètres avancés du proxy FTP :

Propriété	Description
Control Connection Timeouts (Délais d'expiration des connexion de données)	Nombre maximal de secondes pendant lesquelles le proxy FTP attend davantage de communications dans la connexion de contrôle de la part d'un client FTP ou d'un serveur FTP inactif lorsque la transaction en cours n'est pas terminée. • **Client side** (Côté client). Valeur de délai d'expiration pour les connexions de contrôle vers les clients FTP inactifs. • **Server side** (Côté serveur). Valeur de délai d'expiration pour les connexions de contrôle aux serveurs FTP inactifs.
Data Connection Timeouts (Délais d'expiration des connexions de données)	Temps pendant lequel le proxy FTP attend davantage de communications dans la connexion de données à partir d'un client FTP ou d'un serveur FTP inactif lorsque la transaction en cours n'est pas terminée. • **Client side** (Côté client). Valeur du délai d'expiration des connexions de données vers les clients FTP inactifs. • **Server side** (Côté serveur). Valeur du délai d'expiration des connexions de données aux serveurs FTP inactifs.

Étape 5 Envoyez et validez vos modifications.

What to do next

- Survol des services proxy FTP, on page 92

Services proxy SOCKS

Survol des services de proxy SOCKS

Le Secure Web Appliance inclut un proxy SOCKS pour traiter le trafic SOCKS. Les politiques SOCKS sont l'équivalent des politiques d'accès qui contrôlent le trafic SOCKS. Tout comme les politiques d'accès, vous pouvez utiliser les profils d'identification pour indiquer les transactions qui sont régies par chaque politique SOCKS. Une fois que les politiques SOCKS sont appliquées aux transactions, les politiques de routage peuvent régir le routage du trafic.

Notez les éléments suivants concernant le proxy SOCKS :

- Le protocole SOCKS prend uniquement en charge les connexions directes.
- Le proxy SOCKS ne prend pas en charge les proxys en amont (ne transmettra pas à ces derniers).
- Le proxy SOCKS ne prend pas en charge les services d'analyse, qui sont utilisés par Application Visibility and Control (AVC), la Prévention de la perte de données (DLP) et la détection des programmes malveillants.
- Le proxy SOCKS ne prend pas en charge le traçage des politiques.
- Le proxy SOCKS ne déchiffre pas le trafic SSL; il effectue la tunnelisation du client vers le serveur.

Activation du traitement du trafic SOCKS

Before you begin

Activez le proxy Web.

Étape 1 Choisissez **Security Services** > **SOCKS Proxy** (Services de sécurité > Proxy SOCKS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Enable SOCKS Proxy** (Activer le proxy SOCKS).

Étape 4 **Envoyez** et **validez** les modifications.

Configuration du serveur proxy SOCKS

Étape 1 Choisissez **Security Services** > **SOCKS Proxy** (Services de sécurité > SOCKS > Proxy).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Enable SOCKS Proxy** (Activer le proxy SOCKS).

Étape 4 Configurez les paramètres de base et avancés du proxy SOCKS.

Proxy SOCKS	Activé.
SOCKS Control Ports (Ports de contrôle SOCKS)	Ports qui acceptent les demandes SOCKS. La valeur par défaut est 1080.

UDP Request Ports (Ports de demande UDP)	Ports UDP sur lesquels le serveur SOCKS doit écouter. La valeur par défaut est 16000-16100.
Proxy Negotiation Timeout (Délai d'expiration de la négociation du proxy)	Temps d'attente (en secondes) avant d'envoyer ou de recevoir des données d'un client SOCKS dans la phase de négociation. La valeur par défaut est 60.
UDP Tunnel Timeout (Délai d'expiration du tunel UDP)	Temps d'attente (en secondes) des données d'un client ou d'un serveur UDP avant de fermer le tunnel UDP. La valeur par défaut est 60.

Création des politiques SOCKS

Étape 1 Choisissez **Web Security Manager** > **SOCKS Policies** (Web Security Manager > Politiques SOCKS).

Étape 2 Cliquez sur **Add Policy** (Ajouter une politique).

Étape 3 Attribuez un nom dans le champ **Policy Name** (Nom de la politique).

Note Chaque nom de groupe de politiques doit être unique et contenir uniquement des caractères alphanumériques ou un espace.

Étape 4 (Facultatif) Ajoutez une description.

Étape 5 Dans le champ **Insert Above Policy** (Insérer au-dessus de la politique), choisissez l'endroit dans la table des politiques SOCKS où insérer cette politique SOCKS.

Note Lorsque vous configurez plusieurs politiques SOCKS, déterminez un ordre logique pour chaque politique. Ordonnez vos politiques pour vous assurer que la correspondance est correcte.

Étape 6 Dans la section **Identity and Users** (Identités et utilisateurs), choisissez une ou plusieurs identités à appliquer à ce groupe de politiques.

Étape 7 (Facultatif) Développez la section « Advanced » (Avancé) pour définir les exigences d'appartenance supplémentaires.

Proxy Ports (Ports du proxy)	Le port configuré dans le navigateur. (Facultatif) Définissez l'appartenance au groupe de politiques par le port de proxy utilisé pour accéder au proxy Web. Entrez un ou plusieurs numéros de port dans le champ Proxy Ports (Ports du proxy). Séparez les valeurs de ports multiples par des virgules. Vous pouvez définir l'appartenance à un groupe de politiques sur le port du proxy, si un ensemble de clients est configuré pour transférer explicitement les demandes sur un port et un autre ensemble de clients est configuré pour transférer explicitement les demandes sur un port différent. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques SOCKS.

Subnets (Sous-réseaux)	(Facultatif) Définissez l'appartenance au groupe de politiques par sous-réseau ou autres adresses. Vous pouvez choisir d'utiliser les **adresses** qui peuvent être **définies** avec l'**identité** associée ou vous pouvez entrer des **adresses spécifiques** ici. **Note** Si l'identité associée à ce groupe de politiques définit ses membres par des adresses, dans ce groupe de politiques, vous devez saisir des adresses qui constituent un sous-ensemble des adresses de l'identité. L'ajout d'adresses dans le groupe de politiques réduit davantage la liste des transactions qui correspondent à ce groupe de politiques.
Time Range (Plage de temps)	(Facultatif) Définir l'appartenance au groupe de politiques par plage de temps : **a.** Sélectionnez une plage de temps dans le champ **Time Range** (Plage de temps). **b.** Indiquez si ce groupe de politiques doit s'appliquer aux heures à l'intérieur ou à l'extérieur de la plage de temps sélectionnée.

Étape 8 Envoyez et validez les modifications.

What to do next

- (Facultatif) Ajoutez une identité à utiliser avec les politiques SOCKS.
- Ajoutez une ou plusieurs politiques SOCKS pour gérer le trafic SOCKS.

Cisco Umbrella Seamless ID

La fonctionnalité Cisco Umbrella Seamless ID permet à l'appliance de transmettre les informations d'identification de l'utilisateur à Cisco Umbrella Secure Web Gateway (SWG) après une authentification réussie. Cisco Umbrella SWG vérifie les informations de l'utilisateur dans Active Directory en fonction des informations d'identification authentifiées reçues de Secure Web Appliance. Cisco Umbrella SWG considère l'utilisateur comme authentifié et lui fournit un accès en fonction des politiques de sécurité définies.

Secure Web Appliance transmet les informations d'identification de l'utilisateur à Cisco Umbrella SWG à l'aide des en-têtes HTTP; X-USWG-PKH, X-USWG-SK et X-USWG-Data.

Remarque

- Les en-têtes Cisco Umbrella Seamless ID remplacent les en-têtes avec le même nom sur Secure Web Appliance, le cas échéant.
- La fonctionnalité Cisco Umbrella Seamless ID prend en charge le schéma d'authentification auprès d'Active Directory uniquement. Cette fonctionnalité ne prend pas en charge LDAP, Cisco Identity Services Engine (ISE) et l'agent Cisco Context Directory (CDA).
- Cisco Umbrella SWG ne prend pas en charge le trafic FTP et SOCKS.

Tableau 3 : Comportement du trafic HTTPs

Mode de déploiement	Méthode de substitution	Decrypt for Authentication (Déchiffrer pour authentification)	Authentification Secure Web Appliance	Partage Cisco Umbrella Seamless ID
Explicite	Substitution d'IP	Oui/Non	Oui	Oui
Transparent	Substitution d'IP	Oui	Oui	Oui
Transparent	Substitution d'IP	Non	Ignore l'authentification	Non
Explicite	Témoin, sans chiffrement des identifiants	Oui/Non	Oui	Oui
Explicite	Témoin, avec chiffrement des identifiants	Oui/Non	Oui	Non
Transparent	Témoin avec/sans chiffrement des identifiants	Oui/Non	Ignore l'authentification	Non

Remarque Secure Web Appliance récupère la valeur UPN pour l'utilisateur authentifié à partir d'Active Directory et permet à Cisco Umbrella Seamless ID d'appliquer les politiques Web correctes pour les utilisateurs. Pour que cette fonctionnalité soit opérante, vous devez affecter à tous les utilisateurs Active Directory des valeurs UPN par défaut ou personnalisées.

Cette section aborde les points suivants :

- Configuration de Cisco Umbrella Seamless ID
- Configuration de la destination de routage pour Cisco Umbrella SWG

Configuration de Cisco Umbrella Seamless ID

Avant de commencer

- Chargez manuellement le certificat racine ou Cisco Umbrella personnalisé sur l'appliance en sélectionnant **Network** > **Certificate Management** > **Manage Trusted Root Certificates**(Réseau > Gestion des certificats > Gérer les certificats racine approuvés). Voir Certificate Management.
- Assurez-vous d'avoir configuré les profils d'identification pour l'authentification.
- Définissez des politiques de routage avec des profils d'identification configurés.

Étape 1 Choisissez **Web Security Manager** > **Cisco Umbrella Seamless ID** .

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Saisissez l'adresse IP ou le nom d'hôte Cisco Umbrella SWG.

Étape 4 Entrez les numéros de port du SWG pour le trafic HTTP et HTTPS.

Vous pouvez saisir au maximum six numéros de port.

Étape 5 (Facultatif) Cliquez sur **Connectivity Test** (Test de connectivité) pour vérifier la connectivité de Cisco Umbrella SWG sur les ports et la validation des certificats.

Étape 6 Entrez l'ID unique d'organisation du client de Cisco Umbrella SWG.

Étape 7 Envoyez et validez.

Configuration de la destination de routage pour Cisco Umbrella SWG

Pour créer une nouvelle politique de routage, consultez Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage

.

Étape 1 Choisissez **Web Security Manager** > **Routing Policies** (Web Security Manager > Politiques de routage).

Étape 2 Dans la page **Routing Policies** (Politiques de routage), cliquez sur le lien dans la colonne **Routing Destination** (Destination de routage) correspondant à la politique de routage dont vous souhaitez configurer le Cisco Umbrella Seamless ID avec le port requis.

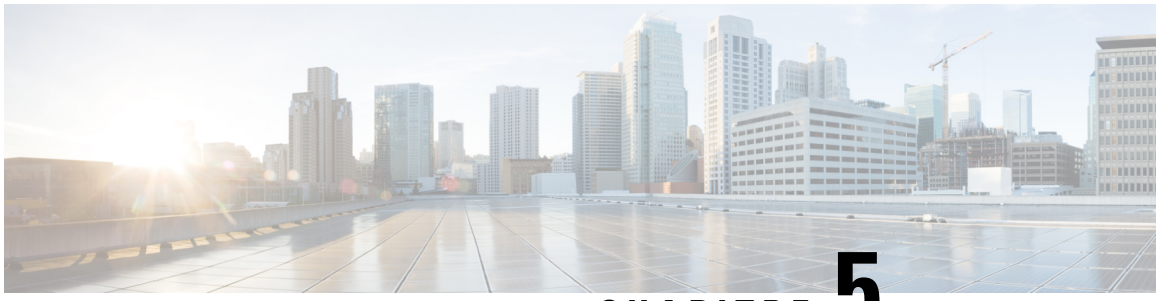
Étape 3 Sélectionnez le Cisco Umbrella Seamless ID approprié avec port comme groupe de proxys en amont pour la politique. La liste déroulante Upstream Proxy Group (Groupe de proxys en amont) affiche tous les Cisco Umbrella Seamless ID avec ports que vous avez configurés dans la page **Cisco Umbrella Seamless ID** (**Web Security Manager** > **Cisco Umbrella Seamless ID**).

Remarque Si vous supprimez un **Cisco Umbrella Seamless ID** avec un numéro de port (**Web Security Manager** > **Cisco Umbrella Seamless ID**) déjà associé à une politique de routage, la destination du routage est automatiquement remplacée par « Direct Connection » (Connexion directe).

Étape 4 Envoyez et validez vos modifications.

Résolution de problèmes de demandes d'interception

- Les catégories d'URL ne bloquent pas certains sites FTP, on page 639
- Déconnexion des transferts FTP volumineux, on page 639
- Le fichier de zéro octet apparaît sur les serveurs FTP après le chargement du fichier, on page 639
- Unable to Route FTP Requests Via an Upstream Proxy (Impossible d'acheminer les requêtes FTP de la voie de routage par le biais d'un proxy en amont), on page 660
- Les demandes HTTPS et FTP via HTTP correspondent uniquement aux politiques d'accès qui ne nécessitent pas d'authentification, on page 652
- Politique globale de correspondances des utilisateurs pour les demandes HTTPS et FTP via HTTP, on page 653



CHAPITRE 5

Acquérir les informations d'authentification de l'utilisateur final

Cette rubrique contient les sections suivantes :

Survol de l'acquisition des informations d'authentification de l'utilisateur final

Type de serveur/domaine	Schéma d'authentification	Protocole réseau pris en charge	Notes
Active Director	Kerberos NTLMSSP Basic (niveau de base)	HTTP, HTTPS FTP natif, FTP sur HTTP SOCKS (Authentification de base)	Kerberos n'est pris en charge qu'en mode standard. Il n'est pas pris en charge en mode Cloud Connector.
LDAP	Basic (niveau de base)	HTTP, HTTPS FTP natif, FTP sur HTTP SOCKS	—

Survol des tâches d'authentification

Étape	Tâche	Liens vers des rubriques et des procédures connexes
1	Créez un domaine d'authentification.	• Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique), on page 122 • Création d'un domaine d'authentification LDAP, on page 125
2	Configurez des paramètres d'authentification globaux.	• Configuration des paramètres d'authentification globaux, on page 131
3	Configurez l'authentification extérieure. Vous pouvez authentifier les utilisateurs au moyen d'un serveur LDAP ou RADIUS externe.	• Authentification extérieure, on page 116
4	(Facultatif) Créez et organisez des domaines d'authentification supplémentaires. Créez au moins un domaine d'authentification pour chaque combinaison de protocole et de schéma d'authentification que vous prévoyez d'utiliser.	• Création de séquences d'authentification, on page 140
5	(Facultatif) Configurez le chiffrement des informations d'authentification.	• Configuration du chiffrement des informations d'authentification, on page 149
6	Créer des profils d'identification pour classer les utilisateurs et les logiciels clients en fonction des exigences d'authentification.	• Classification des utilisateurs et logiciels clients, on page 153
7	Créez des politiques pour gérer les demandes Web provenant des utilisateurs et groupes d'utilisateurs pour lesquels vous avez créé des profils d'identification.	• Bonnes pratiques en matière de gestion des demandes Web au moyen de politiques, on page 249

Bonnes pratiques en matière d'authentification

- Créez aussi peu de domaines Active Directory que possible. Plusieurs domaines Active Directory nécessitent une utilisation de mémoire supplémentaire pour l'authentification.
- Si vous utilisez NTLMSSP, authentifiez les utilisateurs à l'aide de Secure Web Appliance ou du serveur proxy en amont, mais pas des deux. (Recommander Secure Web Appliance)
- Si vous utilisez Kerberos, authentifiez-vous à l'aide de Secure Web Appliance.
- Pour des performances optimales, authentifiez les clients sur le même sous-réseau à l'aide d'un seul domaine.

- Certains agents utilisateurs sont connus pour avoir des problèmes avec les informations d'authentification de l'ordinateur ou des échecs d'authentification, ce qui peut avoir une incidence négative sur leurs opérations normales. Vous devez contourner l'authentification avec ces agents utilisateurs. Consultez Contournement de l'authentification avec des agents utilisateur problématiques , on page 142.
- L'authentification active d'un client est une tâche exigeante en ressources. Les substitutions d'authentification peuvent être utilisées pour améliorer les performances d'authentification en se souvenant d'un utilisateur authentifié pendant un certain temps (par défaut 3600 secondes et configurable dans [**Global Authentication** > **Surrogate Timeout** (Authentification globale > Expiration des substitutions)]) une fois l'authentification terminée. Les substitutions IP doivent être utilisées chaque fois que possible pour limiter le nombre d'événements d'authentification actifs.

Planification de l'authentification

Active Directory/Kerberos

Renvoi explicite	Mise en cache transparente basée sur IP	Mise en cache transparente basée sur les témoins
Avantages : • Performance et interopérabilité améliorées par rapport à NTLM • Fonctionne avec les clients Windows et non Windows qui ont rejoint le domaine • Pris en charge par tous les navigateurs et la plupart des autres applications • Basé sur les RFC • Surcharge minimale (la réauthentification n'est pas requise) • Fonctionne pour les demandes HTTPS (CONNECT) • Comme la phrase secrète n'est pas transmise au serveur d'authentification, elle est encore plus sécurisée • La connexion est authentifiée, pas l'hôte ou l'adresse IP • Réalise une véritable connexion unique dans un environnement Active Directory lorsque les applications clientes sont configurées pour faire confiance au Secure Web Appliance	**Avantages :** • Performance et interopérabilité améliorées par rapport à NTLM • Fonctionne avec les clients Windows et non Windows qui ont rejoint le domaine • Fonctionne avec tous les principaux navigateurs • Pour le cas des agents utilisateur qui ne prennent pas en charge l'authentification, les utilisateurs doivent seulement s'authentifier dans un navigateur pris en charge. • Surdébit relativement faible • Fonctionne pour les demandes HTTPS si l'utilisateur s'est déjà authentifié avec une requête HTTP	**Avantages** : • Performance et interopérabilité améliorées par rapport à NTLM • Fonctionne avec les clients Windows et non Windows qui ont rejoint le domaine • Fonctionne avec tous les principaux navigateurs • L'authentification est associée à l'utilisateur plutôt qu'à l'hôte ou à l'adresse IP **Inconvénients** : • Chaque nouveau domaine Web nécessite l'ensemble du processus d'authentification, car les témoins sont propres au domaine • Nécessite l'activation des témoins • Ne fonctionne pas pour les demandes HTTPS

Active Directory/Basique

Renvoi explicite	Mise en cache transparente basée sur IP	Mise en cache transparente basée sur les témoins
Avantages : • Pris en charge par tous les navigateurs et la plupart des autres applications • Basé sur les RFC • Surcharge minimale • Fonctionne pour les demandes HTTPS (CONNECT) • Comme la phrase secrète n'est pas transmise au serveur d'authentification, elle est encore plus sécurisée • La connexion est authentifiée, pas l'hôte ou l'adresse IP • Réalise une véritable connexion unique dans un environnement Active Directory lorsque les applications clientes sont configurées pour faire confiance au Secure Web Appliance **Inconvénients** : • Phrase secrète envoyée en texte clair (Base64) pour chaque demande • Absence de connexion unique • Surdébit modéré : chaque nouvelle connexion doit être réauthentifiée • Principalement pris en charge sur Windows uniquement et avec les principaux navigateurs uniquement	**Avantages :** • Fonctionne avec tous les principaux navigateurs • Pour le cas des agents utilisateur qui ne prennent pas en charge l'authentification, les utilisateurs doivent seulement s'authentifier dans un navigateur pris en charge. • Surdébit relativement faible • Fonctionne pour les demandes HTTPS si l'utilisateur s'est déjà authentifié avec une requête HTTP **Inconvénients** : • Les informations d'authentification sont associées à l'adresse IP, pas à l'utilisateur (ne fonctionne pas dans les environnements Citrix et RDP ou si l'utilisateur change d'adresse IP) • Absence de connexion unique • La phrase secrète est envoyée en texte clair (Base64)	**Avantages** : • Fonctionne avec tous les principaux navigateurs • L'authentification est associée à l'utilisateur plutôt qu'à l'hôte ou à l'adresse IP **Inconvénients** : • Chaque nouveau domaine Web nécessite l'ensemble du processus d'authentification, car les témoins sont propres au domaine • Nécessite l'activation des témoins • Ne fonctionne pas pour les demandes HTTPS • Absence de connexion unique • La phrase secrète est envoyée en texte clair (Base64)

Active Directory/NTLMSSP

Renvoi explicite	Transparent
Avantages : • Comme la phrase secrète n'est pas transmise au serveur d'authentification, elle est encore plus sécurisée • La connexion est authentifiée, pas l'hôte ou l'adresse IP • Réalise une véritable connexion unique dans un environnement Active Directory lorsque les applications clientes sont configurées pour faire confiance au Secure Web Appliance **Inconvénients :** • Surdébit modéré : chaque nouvelle connexion doit être réauthentifiée • Principalement pris en charge sur Windows uniquement et avec les principaux navigateurs uniquement	**Avantages :** • Plus de flexibilité L'authentification NTLMSSP transparente est similaire à l'authentification de base transparente, sauf que le proxy Web communique avec les clients à l'aide d'un processus de test-réponse au lieu du nom d'utilisateur et de la phrase secrète de base en texte clair. Les avantages et les inconvénients de l'authentification MSTN transparente sont les mêmes que ceux de l'authentification de base transparente, sauf qu'elle présente l'avantage supplémentaire de ne pas envoyer de phrase secrète au serveur d'authentification et que vous pouvez réaliser une connexion unique lorsque les applications clientes sont configurées pour faire confiance à Secure Web Appliance**.**

LDAP/Basic

Renvoi explicite	Transparent
Avantages : • Basé sur les RFC • Davantage de navigateurs pris en charge que NTLM • Surcharge minimale • Fonctionne pour les demandes HTTPS (CONNECT) **Inconvénients :** • Absence de connexion unique • Phrase secrète envoyée en texte clair (Base64) pour chaque demande **Solutions :** • Échec de l'authentification, on page 141	**Avantages :** • Plus flexible que le renvoi explicite. • Davantage de navigateurs pris en charge que NTLM • Pour le cas des agents utilisateur qui ne prennent pas en charge l'authentification, les utilisateurs doivent seulement s'authentifier dans un navigateur pris en charge. • Surdébit relativement faible • Fonctionne pour les demandes HTTPS si l'utilisateur s'est déjà authentifié avec une requête HTTP **Inconvénients :** • Absence de connexion unique • La phrase secrète est envoyée en texte clair (Base64) • Les informations d'authentification sont associées à l'adresse IP, pas à l'utilisateur (ne fonctionne pas dans les environnements Citrix et RDP ou si l'utilisateur change d'adresse IP) **Solutions :** • Échec de l'authentification, on page 141

Identification transparente des utilisateurs

Habituellement, les utilisateurs sont identifiés et authentifiés en les invitant à saisir un nom d'utilisateur et une phrase secrète. Ces informations d'authentification sont validées par rapport à un serveur d'authentification, puis le proxy Web applique les politiques appropriées à la transaction en fonction du nom d'utilisateur authentifié.

Cependant, vous pouvez configurer Secure Web Appliance pour authentifier les utilisateurs de manière transparente, c'est-à-dire sans demander à l'utilisateur final de fournir ses informations d'authentification. L'identification transparente authentifie l'utilisateur au moyen d'informations d'authentification obtenues à partir d'une autre source de confiance, en supposant que l'utilisateur a déjà été authentifié par cette source de confiance, puis applique les politiques appropriées.

Vous pourriez souhaiter identifier les utilisateurs de manière transparente pour :

- Créer un environnement de connexion unique de sorte que les utilisateurs ne soient pas informés de la présence d'un proxy sur le réseau.
- Appliquer des politiques basées sur l'authentification aux transactions émanant d'applications clientes qui sont incapables d'afficher une invite d'authentification aux utilisateurs finaux.

L'identification transparente des utilisateurs affecte uniquement la façon dont le proxy Web obtient le nom d'utilisateur et attribue un profil d'identification. Après avoir obtenu le nom d'utilisateur et attribué un profil d'identification, il applique normalement toutes les autres politiques, quelle que soit la façon dont il a attribué le profil d'identification.

Si l'authentification transparente échoue, vous pouvez configurer le traitement de la transaction : vous pouvez accorder à l'utilisateur un accès invité ou forcer l'affichage d'une invite d'authentification à l'attention de l'utilisateur.

Lorsqu'une invite d'authentification apparaît à un utilisateur final en raison d'un échec de l'identification transparente de l'utilisateur et que l'authentification échoue en raison d'informations d'authentification non valides, vous pouvez choisir d'autoriser ou non l'accès de l'utilisateur invité.

Note Lorsque vous activez la réauthentification et qu'une transaction est bloquée par le filtrage d'URL, une page de notification à l'utilisateur final s'affiche avec l'option de connexion sous un autre nom d'utilisateur. Les utilisateurs qui cliquent sur le lien sont invités à s'authentifier. Pour en savoir plus, consultez Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes, on page 145.

Comprendre l'identification transparente de l'utilisateur

Les méthodes disponibles pour l'identification transparente de l'utilisateur sont les suivantes :

- **Transparently identify users with ISE** (Identifier en toute transparence les utilisateurs avec ISE) : disponible lorsque le service de moteur de services de vérification des identités (ISE) ou du connecteur d'identité passif (ISE-PIC) est activé [Network > Identity Services Engine (Réseau > Moteur ISE)]. Pour ces transactions, le nom d'utilisateur et les étiquettes Groupe sécurisé associées seront obtenus à partir d'un serveur de moteur de services d'identité. Si vous utilisez ISE-PIC, on obtiendra le nom d'utilisateur et les groupes ISE Secure associés. Consultez Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 177.
- **Transparently identify users with ASA** (Identification transparente des utilisateurs avec ASA) : les utilisateurs sont identifiés par le mappage adresse IP actuel-nom d'utilisateur reçu d'une appliance Cisco Adaptive Security Appliance (pour les utilisateurs à distance seulement). Cette option est disponible lorsqu'AnyConnect Secure Mobility est activé et intégré à un ASA. Le nom d'utilisateur sera obtenu auprès de l'ASA, et les groupes d'annuaires associés seront obtenus à partir du domaine ou de la séquence d'authentification précisée sur la Secure Web Appliance. Consultez Utilisateurs à distance, on page 274.
- **Transparently identify users with authentication realms** (Identification transparente des utilisateurs avec des domaines d'authentification) : cette option est disponible lorsqu'un ou plusieurs domaines d'authentification sont configurés pour prendre en charge l'identification transparente à l'aide de l'un des serveurs d'authentification suivants :
  - **Active Directory** : crée un domaine d'authentification NTLM ou Kerberos et active une identification transparente des utilisateurs. En outre, vous devez déployer un agent Active Directory distinct comme l'agent Context Directory de Cisco. Pour en savoir plus, consultez Identification transparente de l'utilisateur avec Active Directory, on page 109.
  - **LDAP** : crée un domaine d'authentification LDAP configuré comme un eDirectory et active une identification transparente des utilisateurs. Pour en savoir plus, consultez Identification transparente de l'utilisateur avec LDAP, on page 110.

AsyncOS pour le Web communique à des intervalles réguliers avec eDirectory ou un agent Active Directory pour maintenir les mappages qui font correspondre les noms d'utilisateurs authentifiés à leurs adresses IP actuelles.

Identification transparente de l'utilisateur avec Active Directory

Active Directory n'enregistre pas les informations de connexion de l'utilisateur dans un format permettant aux autres systèmes d'interroger facilement d'autres systèmes, par exemple Secure Web Appliance. Les agents Active Directory, tels que l'agent Context Directory Agent (CDA) de Cisco, sont nécessaires pour interroger les journaux des événements de sécurité Active Directory pour obtenir des renseignements sur les utilisateurs authentifiés.

Note CDA n'est pas pris en charge par Active Directory dans Windows Server 2016. Vous pouvez utiliser le service ISE (Identity Services Engine - Moteur du service de vérification des identités) ou ISE-PIC (ISE Passive Identity Controller) pour recevoir les informations de l'utilisateur et obtenir une identification transparente de l'utilisateur. Vous devez configurer les profils d'identification et les politiques d'accès pertinentes, ainsi que les politiques de déchiffrement qui utilisent CDA, avec les informations ISE/ISE-PIC lorsque vous passez de CDA à ISE/ISE-PIC.

AsyncOS pour le Web communique avec l'agent Active Directory pour conserver une copie locale des mappages adresse IP-nom d'utilisateur. Quand AsyncOS pour le Web doit associer une adresse IP à un nom d'utilisateur, il vérifie d'abord sa copie locale des mappages. Si aucune correspondance n'est trouvée, il interroge un agent Active Directory pour trouver une correspondance.

Pour en savoir plus sur l'installation et la configuration d'un agent Active Directory, consultez la section « Configuration d'un agent Active Directory pour fournir des informations à Secure Web Appliance » ci-dessous.

Prenez en compte les éléments suivants lorsque vous identifiez les utilisateurs de manière transparente à l'aide d'Active Directory :

- L'identification transparente des utilisateurs avec Active Directory fonctionne uniquement avec un schéma d'authentification NTLM ou Kerberos. Vous ne pouvez pas l'utiliser avec un domaine d'authentification LDAP qui correspond à une instance Active Directory.
- L'identification transparente de l'utilisateur fonctionne avec les versions d'Active Directory prises en charge par un agent Active Directory.
- Vous pouvez installer une deuxième instance d'un agent Active Directory sur un autre ordinateur pour atteindre une disponibilité élevée. Lorsque vous faites cela, chaque agent Active Directory gère les mappages de l'adresse IP au nom d'utilisateur indépendamment de l'autre agent. AsyncOS pour le Web utilise l'agent Active Directory de secours après trois tentatives ping infructueuses vers l'agent principal.
- L'agent Active Directory utilise le mode à la demande lorsqu'il communique avec Secure Web Appliance.
- L'agent Active Directory envoie les informations de déconnexion de l'utilisateur vers Secure Web Appliance. Parfois, certaines informations de déconnexion d'utilisateurs ne sont pas enregistrées dans les journaux de sécurité Active Directory. Cela peut se produire si l'ordinateur client tombe en panne ou si l'utilisateur éteint l'appareil sans se déconnecter. Si les journaux de sécurité ne contiennent aucune information de déconnexion de l'utilisateur, un agent Active Directory ne peut pas informer l'appliance que l'adresse IP n'est plus attribuée à cet utilisateur. Pour éviter cette possibilité, vous pouvez définir pendant combien de temps AsyncOS met en cache les mappages adresse IP-utilisateur lorsqu'il n'y a aucune mise à jour d'un agent Active Directory. Pour en savoir plus, consultez Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur, on page 112.

- L'agent Active Directory enregistre le nom `sAMAccountName` de chaque utilisateur se connectant à partir d'une adresse IP particulière afin de s'assurer que le nom d'utilisateur est unique.
- Les adresses IP des clients que les ordinateurs clients présentent au serveur Active Directory et au Secure Web Appliance doivent être identiques.
- AsyncOS pour le Web recherche uniquement les groupes parents directs pour un utilisateur. Il ne recherche pas les groupes imbriqués.

Configuration d'un agent Active Directory pour fournir des informations à Secure Web Appliance

Comme AsyncOS pour le Web ne peut pas obtenir les adresses IP des clients directement à partir d'Active Directory, il doit obtenir les informations de mappage adresse IP-nom d'utilisateur auprès d'un agent Active Directory.

Installez un agent Active Directory sur un ordinateur du réseau qui est accessible à Secure Web Appliance et qui peut communiquer avec tous les contrôleurs de domaine Windows visibles. Pour de meilleures performances, cet agent doit être physiquement aussi proche que possible de Secure Web Appliance. Dans les environnements réseau plus petits, vous pouvez installer l'agent Active Directory directement sur le serveur Active Directory.

Note L'instance de l'agent Active Directory utilisée pour communiquer avec Secure Web Appliance peut également prendre en charge d'autres appliances, y compris l'appliance ASA (Adaptive Security Appliance) de Cisco et d'autres Secure Web Appliance.

Obtention, installation et configuration de l'agent Context Directory Agent de Cisco

Pour en savoir plus sur le téléchargement, l'installation et la configuration de l'agent Cisco Context Directory, consultez l'adresse suivante :
http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html.

Note Secure Web Appliance et l'agent Active Directory communiquent à l'aide du protocole RADIUS. L'appliance et l'agent doivent être configurés avec le même secret partagé pour brouiller les phrases secrètes des utilisateurs. Les autres attributs utilisateur ne sont pas masqués.

Identification transparente de l'utilisateur avec LDAP

AsyncOS pour le Web peut communiquer avec un serveur eDirectory configuré comme domaine LDAP (Lightweight Directory Access Protocol) en maintenant les mappages de l'adresse IP sur le nom d'utilisateur. Lorsqu'un utilisateur se connecte par l'intermédiaire d'un client eDirectory, il est authentifié sur le serveur eDirectory. Une fois l'authentification réussie, l'adresse IP du client est enregistrée sur le serveur eDirectory en tant qu'attribut (NetworkAddress) de l'utilisateur qui s'est connecté.

Tenez compte des éléments suivants lorsque vous identifiez les utilisateurs de manière transparente à l'aide de LDAP (eDirectory) :

- Le client eDirectory doit être installé sur chaque poste de travail client et les utilisateurs finaux doivent l'utiliser pour s'authentifier sur un serveur eDirectory.

- L'arborescence LDAP utilisée par la connexion du client eDirectory doit être la même que celle configurée dans le domaine d'authentification.
- Si les clients eDirectory utilisent plusieurs arborescences LDAP, créez un domaine d'authentification pour chaque arborescence, puis créez une séquence d'authentification qui utilise chaque domaine d'authentification LDAP.
- Lorsque vous configurez le domaine d'authentification LDAP en tant que domaine eDirectory, vous devez préciser un ND de liaison pour les informations d'authentification de requête.
- Le serveur eDirectory doit être configuré pour mettre à jour l'attribut NetworkAddress de l'objet utilisateur lorsqu'un utilisateur se connecte.
- AsyncOS pour le Web recherche uniquement les groupes parents directs pour un utilisateur. Il ne recherche pas les groupes imbriqués.
- Vous pouvez utiliser l'attribut NetworkAddress pour un utilisateur eDirectory afin de déterminer l'adresse IP de connexion la plus récente de l'utilisateur.

Règles et directives pour une identification transparente de l'utilisateur

Tenez compte des règles et directives suivantes lorsque vous utilisez une identification transparente de l'utilisateur avec un serveur d'authentification :

- Lorsque vous utilisez DHCP pour affecter des adresses IP aux ordinateurs clients, vérifiez que les mappages adresse IP-nom d'utilisateur sont mis à jour sur Secure Web Appliance plus fréquemment que le bail DHCP. Utilisez la commande de l'interface de ligne de commande `tuiconfig` pour mettre à jour l'intervalle de mise à jour du mappage. Pour en savoir plus, consultez Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur, on page 112.
- Si un utilisateur se déconnecte d'une appliance et qu'un autre utilisateur se connecte à la même appliance avant la mise à jour du mappage adresse IP-nom d'utilisateur sur le Secure Web Appliance, le proxy Web connecte le client en tant qu'utilisateur précédent.
- Vous pouvez configurer la façon dont le proxy Web traite les transactions en cas d'échec de l'identification transparente de l'utilisateur. Il peut accorder aux utilisateurs un accès invité ou forcer l'affichage d'une invite d'authentification pour les utilisateurs finaux.
- Lorsqu'une invite d'authentification s'affiche en raison d'un échec de l'identification transparente de l'utilisateur et que l'authentification échoue en raison de l'échec de l'identification transparente de l'utilisateur, vous pouvez choisir d'autoriser ou non l'accès de l'utilisateur en tant qu'invité.
- Lorsque le profil d'identification attribué utilise une séquence d'authentification avec plusieurs domaines dans lesquels l'utilisateur existe, AsyncOS pour le Web récupère les groupes d'utilisateurs des domaines dans l'ordre dans lequel ils apparaissent dans la séquence.
- Lorsque vous configurez un profil d'identification pour identifier les utilisateurs de manière transparente, le modèle d'authentification doit être l'adresse IP. Vous ne pouvez pas sélectionner un type de substitution différent.
- Lorsque vous affichez le détail des transactions pour les utilisateurs, la page de suivi Web indique quels utilisateurs ont été identifiés de manière transparente.
- Vous pouvez consigner les utilisateurs qui ont été identifiés de manière transparente dans les journaux d'accès et WC3 à l'aide des champs personnalisés `%m` et `x-auth-mecanism`. Une entrée de journal `SSO_TUI` indique que le nom d'utilisateur a été obtenu en faisant correspondre l'adresse IP du client à un nom d'utilisateur authentifié à l'aide d'une identification transparente de l'utilisateur. (De même, la valeur

`SSO_ASA` indique que l'utilisateur est un utilisateur distant et que le nom d'utilisateur a été obtenu auprès d'un Cisco ASA à l'aide d'AnyConnect Secure Mobility.)

Configuration de l'identification transparente de l'utilisateur

La configuration de l'identification et de l'autorisation transparentes des utilisateurs est décrite en détail dans Survol de l'acquisition des informations d'authentification de l'utilisateur final, on page 101. Les étapes élémentaires sont les suivantes :

- Créer et trier les domaines d'authentification.
- Créer des profils d'identification pour classer les utilisateurs et les logiciels clients.
- Créer des politiques pour gérer les demandes Web émanant des utilisateurs et groupes d'utilisateurs identifiés.

Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur

AsyncOS pour le Web fournit les commandes CLI suivantes liées à l'interface TUI :

- **`tuiconfig`** – Configurez les paramètres avancés associés à l'identification transparente de l'utilisateur. Le mode par lots peut être utilisé pour configurer plusieurs paramètres simultanément.
  - **`Configure mapping timeout for Active Directory agent`** (Configurer le délai d'expiration de mappage pour l'agent Active Directory) : durée, en minutes, pendant laquelle les mappages adresse IP-utilisateur sont mis en cache pour les adresses IP récupérées par l'agent AD quand aucune mise à jour de l'agent n'est effectuée.
  - **`Configure proxy cache timeout for Active Directory agent`** (Configurer le délai d'expiration du cache de proxy pour l'agent Active Directory) : durée, en secondes, pendant laquelle les mappages adresse IP-utilisateur spécifiques au proxy sont mis en cache, en secondes; les valeurs correctes vont de cinq à 1200 secondes. La valeur par défaut et recommandée est de 120 secondes. La définition d'une valeur inférieure peut avoir un impact négatif sur les performances du proxy.
  - **`Configure mapping timeout for Novell eDirectory`** (Configurer le délai de mappage pour Novell eDirectory) : durée, en secondes, pendant laquelle les mappages adresse IP-utilisateur sont mis en cache pour les adresses IP extraites du serveur eDirectory quand aucune mise à jour n'est effectuée à partir du serveur.
  - **`Configure query wait time for Active Directory agent`** (Configurer le temps d'attente de la requête pour l'agent Active Directory) : temps, en secondes, d'attente d'une réponse de l'agent Active Directory. Lorsque la requête prend plus de temps que cette valeur, l'identification transparente de l'utilisateur est considérée comme ayant échoué. Cela limite le délai d'authentification de l'utilisateur final.
  - **`Configure query wait time for Novell eDirectory`** (Configurer le temps d'attente de la requête pour Novell eDirectory) : temps, en secondes, d'attente d'une réponse du serveur eDirectory. Lorsque la requête prend plus de temps que cette valeur, l'identification transparente de l'utilisateur est considérée comme ayant échoué. Cela limite le délai d'authentification de l'utilisateur final.

Les paramètres Active Directory s'appliquent à tous les domaines AD qui utilisent un agent AD pour l'identification transparente de l'utilisateur. Les paramètres eDirectory s'appliquent à tous les domaines LDAP qui utilisent eDirectory pour l'identification transparente des utilisateurs.

Si la validation échoue pour un paramètre, aucune valeur ne sera modifiée.

- **`tuistatus`** : cette commande fournit les sous-commandes liées à AD suivantes :
  - **`adagentstatus`** : affiche l'état actuel de tous les agents AD, ainsi que des informations sur leurs connexions avec les contrôleurs de domaine Windows.
  - **`listlocalmaippings`** : répertorie tous les mappages adresse IP-nom d'utilisateur stockés sur le Secure Web Appliance, tels qu'ils ont été récupérés par le ou les agents AD. Ce paramètre ne répertorie pas les entrées stockées sur le ou les agents, ni les mappages pour lesquels des requêtes sont actuellement en cours.

Configuration de la connexion unique

L'obtention des informations d'authentification facilite la création d'un environnement de connexion unique en toute transparence. L'identification transparente de l'utilisateur est un paramètre du domaine d'authentification.

Pour Internet Explorer, assurez-vous que le nom d'hôte de redirection est le nom d'hôte court (ne contenant pas de points) ou le nom NetBIOS plutôt qu'un domaine qualifié complet. Vous pouvez également ajouter le nom d'hôte de l'appliance à la zone intranet local d'Internet Explorer [Tools > Internet options > Security tab (Outils > options Internet > onglet Sécurité)]. Cependant, cela sera requis sur chaque client. Pour plus d'informations à ce sujet, consultez Comment puis-je configurer correctement NTLM avec SSO (les informations d'authentification envoyées de manière transparente)?

Avec les navigateurs Firefox et d'autres navigateurs autres que Microsoft, les paramètres **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** et **network.automatic-ntlm-auth.trusted-uris** doivent être définis sur le nom d'hôte de redirection en mode transparent. Vous pouvez également vous reporter à Firefox n'envoie pas les informations d'authentification de manière transparente (SSO). Cet article fournit des informations générales sur la modification des paramètres de Firefox.

Pour en savoir plus sur le nom d'hôte de redirection, consultez Configuration des paramètres d'authentification globaux, on page 131 ou la commande d'interface de ligne de commande `sethostname`.

Création d'un compte de service dans Windows Active Directory pour l'authentification Kerberos dans les déploiements à haute disponibilité

Utilisez cette procédure si vous rencontrez des problèmes avec la haute disponibilité avec l'authentification Kerberos. Les scénarios, où des problèmes peuvent survenir lors de l'utilisation de l'authentification Kerberos dans les déploiements à haute disponibilité sont les suivants :

- L'attribut servicePrincipalName du nom d'hôte à haute disponibilité est ajouté à plusieurs comptes d'ordinateurs dans Active Directory.
- L'authentification Kerberos fonctionne si servicePrincipalName a été ajouté au compte d'ordinateur unique dans Active Directory. Lorsque le nœud principal change, la haute disponibilité peut être affectée, car différents nœuds de l'appliance utilisent différentes chaînes de chiffrement pour déchiffrer les tickets de service Keberos.

Avant de commencer

- Choisissez le nom d'utilisateur à utiliser pour la haute disponibilité avec l'authentification Keberos. Nous vous recommandons de créer un nouveau nom d'utilisateur, qui sera utilisé uniquement à cette fin.
- Si vous préférez utiliser un nom d'utilisateur existant :
  - Définissez un mot de passe si le nom d'utilisateur n'en a pas.
  - Dans la boîte de dialogue des propriétés du compte d'utilisateur (dans les utilisateurs et les ordinateurs Active Directory) :

    Assurez-vous que la case User must change password at next logon (L'utilisateur doit changer le mot de passe à la prochaine connexion) n'est pas cochée.

    Cochez la case Password never expires (Le mot de passe n'expire jamais).

Étape 1 Créez un nouveau nom d'utilisateur dans les utilisateurs et les ordinateurs Active Directory.

- Spécifiez un mot de passe.
- Décochez la case User must change password at next logon (L'utilisateur doit changer le mot de passe à la prochaine connexion).
- Cochez la case Password never expires (Le mot de passe n'expire jamais).

Étape 2 Vérifiez si le nom SPN du nom d'hôte à haute disponibilité est associé à l'objet utilisateur Active Directory créé ou choisi. Le SPN se compose d'un préfixe http/ et est suivi du nom d'hôte à haute disponibilité de l'appliance. Assurez-vous que les clients sont en mesure de résoudre le nom d'hôte.

1. Utilisez la commande `setspn -q` dans Windows pour rechercher toute association existante.

   Exemple : `setspn -q http/highavail.com`

   Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance.

2. Supprimez ou ajoutez le SPN en fonction des résultats de la requête :

Remarque Les mots de passe des comptes de service Kerberos à haute disponibilité ne peuvent inclure que des lettres, des chiffres, des espaces et des caractères ~ ! @ # % ^ & () _ - {} ' / [] : ; , | + = * ? <>. Si l'un de ces trois caractères spéciaux « $, ' ou » est utilisé dans le mot de passe du compte de service Kerberos à haute disponibilité, il en résultera un échec lors de la pré-authentification à partir de l'interface utilisateur graphique et de l'interface de ligne de commande. Cependant, l'authentification est réussie pour tous les types de caractères utilisés dans le mot de passe.

Résultat de la requête	Action
Aucun SPN de ce type trouvé.	Associez le nom SPN du nom d'hôte à haute disponibilité associé à l'objet utilisateur Active Directory. • Utilisez la commande `setspn -s` : `setspn -s http/highavail.com hausername` Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance et hausername est le nom d'utilisateur créé ou choisi.

Résultat de la requête	Action
SPN existant trouvé! Le nom commun (CN) indique le nom d'utilisateur créé ou choisi. Exemple : CN = hausername	Aucune autre action n'est nécessaire dans Active Directory.

SPN existant trouvé!
Le nom d'utilisateur usuel (CN) n'affiche pas le nom d'utilisateur créé ou choisi.
	1. Supprimez le SPN.
	Utilisez la commande `setspn -d` :
	`setspn -d http/highavail.com jeandupont`
	Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance et jeandupont est le nom d'utilisateur à dissocier.
	2. Ajoutez le SPN.
	Utilisez la commande `setspn -s` :
	`setspn -s http/highavail.com hausername`
	Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance et hausername est le nom d'utilisateur créé ou choisi.

Remarque Assurez-vous que l'authentification Keytable est activée dans le domaine Active Directory approprié. Consultez Création d'un domaine Active Directory pour le schéma d'authentification Kerberos, à la page 117. Pour les domaines déjà créés, modifiez le domaine et activez l'authentification Keytable.

Domaines d'authentification

Les domaines d'authentification définissent les détails requis pour communiquer avec les serveurs d'authentification et précisent le schéma d'authentification à utiliser lors de la communication avec les clients. AsyncOS prend en charge plusieurs domaines d'authentification. Les domaines peuvent également être regroupés en séquences d'authentification qui permettent aux utilisateurs ayant des exigences d'authentification différentes d'être gérés par les mêmes politiques.

Basculement de l'authentification

La configuration de domaine actuelle comprend un serveur AD ou LDAP principal et deux serveurs de sauvegarde. Si le premier serveur principal n'est pas accessible, la requête atteint le premier serveur de sauvegarde. Si le premier serveur de sauvegarde n'est pas non plus accessible, la requête atteint le deuxième serveur.

Table 4: Temps de basculement à l'aide de la règle IPFW

Temps de basculement	Temps de basculement de la sauvegarde principale à la sauvegarde secondaire en secondes
Pour interrompre la connexion entre l'AD principal et Secure Web Appliance	75 à 80

Temps de basculement	Temps de basculement de la sauvegarde principale à la sauvegarde secondaire en secondes
Pour interrompre la connexion entre l'AD principal et Secure Web Appliance, ainsi que pour interrompre la connexion entre la première sauvegarde et Secure Web Appliance	180 à 250
Redémarrer l'AD principal	42 s
Mettre l'AD principal hors tension	75 à 80
Mettre l'AD principal et le premier serveur de sauvegarde hors tension	180 à 250

Si plusieurs serveurs sont en panne, Secure Web Appliance réessaye d'établir la connexion jusqu'à ce qu'un contrôleur de domaine soit trouvé.

- Authentification extérieure, on page 116
- Création d'un domaine Active Directory pour le schéma d'authentification Kerberos, on page 117
- Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique), on page 122
- Création d'un domaine d'authentification LDAP, on page 125
- À propos de la suppression de domaines d'authentification, on page 130
- Configuration des paramètres d'authentification globaux, on page 131

Thèmes connexes

- Séquences d'authentification, on page 139
- Authentification des utilisateurs RADIUS, on page 583

Authentification extérieure

Vous pouvez authentifier les utilisateurs au moyen d'un serveur LDAP ou RADIUS externe.

Configuration de l'authentification extérieure par l'intermédiaire d'un serveur LDAP

Before you begin

Créez un domaine d'authentification LDAP et configurez-le avec une ou plusieurs requêtes d'authentification extérieure. Création d'un domaine d'authentification LDAP, on page 125.

Étape 1 Activez l'authentification extérieure sur l'appliance :

a) Accédez à **System Administration** > **Users** (Administration système > Utilisateurs).
b) Cliquez sur **Enable** (Activer) dans la section External Authentication (Authentification extérieure).
c) Configurez les options :

Option	Description
Activer l'authentification extérieure	—
Type d'authentification	Sélectionnez LDAP.
External Authentication Cache Timeout (Délai d'expiration du cache d'authentification extérieure)	Nombre de secondes pendant lesquelles AsyncOS stocke les informations d'authentification extérieure avant de recontacter le serveur LDAP pour s'authentifier à nouveau. La valeur par défaut est zéro (0).
Requête d'authentification extérieure LDAP	Une requête configurée avec le domaine LDAP.
Délai d'attente d'une réponse valide du serveur	Le nombre de secondes qu'AsyncOS attend une réponse à la requête du serveur.
Mappage de groupe	Pour chaque nom de groupe dans le répertoire, attribuez un rôle.

Étape 2 Envoyez et validez vos modifications.

Activation de l'authentification extérieure RADIUS

Consultez Activation de l'authentification extérieure à l'aide de RADIUS, on page 584.

Création d'un domaine Active Directory pour le schéma d'authentification Kerberos

Before you begin

- Assurez-vous que l'appliance est configurée en mode standard (et non en mode Cloud Connector).
- Si vous configurez la haute disponibilité, assurez-vous d'avoir également coché la case **Use keytab authentication** (Utiliser l'authentification keytab) dans la section Kerberos High Availability (Haute disponibilité Kerberos) spécifiée à l'**étape 9**.

  Si votre appliance se trouve derrière un périphérique de répartition du trafic HTTP/HTTPS comme un équilibreur de charge, vous devez associer le SPN du périphérique de répartition du trafic dans Active Directory à un compte d'utilisateur et saisir les informations d'authentification de ce compte d'utilisateur dans la section Kerberos High Availability (Haute disponibilité Kerberos). Le SPN du premier périphérique qui redirige le trafic dans la topologie du réseau doit être ajouté. Par exemple, si le trafic réseau sortant des périphériques clients passe par un gestionnaire de trafic, un équilibreur de charge, puis vers Secure Web Appliance, le SPN du gestionnaire de trafic doit être ajouté à un compte d'utilisateur sur Active Directory, et les identifiants de l'utilisateur doivent être saisis dans cette section. En effet, le gestionnaire de trafic est le premier périphérique à rencontrer le trafic des périphériques clients.
- Préparez le serveur Active Directory.
  - Installez Active Directory sur l'un des serveurs suivants : Windows Server 2003, 2008, 2008R2, 2012, 2016 (pour coeus 11.8, 12.0, 12.5, 14.0 et 14.5) ou 2019 (pour coeus 14.5 uniquement).

    Vous pouvez installer le serveur Windows Active Directory 2019 pour coeus 12.5.

- Créez un utilisateur sur le serveur Active Directory :
  - Créez un utilisateur sur le serveur Active Directory qui est membre du groupe des administrateurs de domaine ou des opérateurs de compte.

    Ou

  - Créez un nom d'utilisateur avec les autorisations suivantes :
    - Autorisations Active Directory pour la réinitialisation des mots de passe
    - Écriture validée dans servicePrincipalName
    - Restrictions de compte en écriture
    - Écriture du nom dNShost
    - Écriture dans servicePrincipalName

      Il s'agit des autorisations Active Directory minimales requises par un nom d'utilisateur pour joindre une appliance au domaine et assurer son fonctionnement complet.

- Joignez votre client au domaine. Les clients pris en charge sont Windows XP, Windows 10 et Mac OS 10.5+.
- Utilisez l'outil kerbtray du Kit de ressources Windows pour vérifier le ticket Kerberos sur le client : http://www.microsoft.com/en-us/download/details.aspx?id=17657.
- L'application de visionneuse de tickets sur les clients Mac est disponible dans le menu principal > KeyChain Access (Accès à KeyChain) pour afficher les tickets Kerberos.

- Assurez-vous de disposer des droits et des informations de domaine nécessaires pour joindre le domaine Secure Web Appliance au domaine Active Directory auprès duquel vous souhaitez vous authentifier.
- Comparez l'heure actuelle sur Secure Web Appliance avec l'heure actuelle du serveur Active Directory et vérifiez que la différence n'est pas supérieure à l'heure spécifiée dans l'option « Maximum tolerance for computer clock synchronization » (Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur) sur le serveur Active Directory.
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, soyez prêt à vous assurer que les domaines d'authentification du même nom sur différents Secure Web Appliance ont des propriétés identiques définies sur chaque appliance.
- Configuration de Secure Web Appliance :
  - En mode explicite, le nom d'hôte Secure Web Appliance (commande d'interface de ligne de commande `sethostname`) et le nom de proxy configuré dans le navigateur doivent être identiques.
  - En mode transparent, le nom d'hôte Secure Web Appliance doit être identique au nom d'hôte de redirection (voir Configuration des paramètres d'authentification globaux, on page 131). En outre, le nom d'hôte Secure Web Appliance et le nom d'hôte de redirection doivent être configurés avant la création d'un domaine Keberos.

- Sachez qu'après avoir validé le nouveau domaine, vous ne pouvez pas modifier un protocole d'authentification de domaine.

- Notez que la connexion unique (SSO) doit être configurée sur les navigateurs clients; voir Configuration de la connexion unique, on page 113.
- Pour simplifier l'utilisation des journaux, personnalisez le journal des accès pour utiliser le paramètre de champ personnalisé %m. Consultez Personnalisation des journaux d'accès, on page 523.

Note Les mots de passe des comptes de service Kerberos à haute disponibilité ne peuvent inclure que des lettres, des chiffres, des espaces et des caractères ~ ! @ # % ^ & () _ - {} ' / [] : ; , | + = * ? <>. Si l'un de ces trois caractères spéciaux « $, ' ou » est utilisé dans le mot de passe du compte de service Kerberos à haute disponibilité, il en résultera un échec lors de la pré-authentification à partir de l'interface utilisateur graphique et de l'interface de ligne de commande. Cependant, l'authentification est réussie pour tous les types de caractères utilisés dans le mot de passe.

Étape 1 Dans l'interface Web de Cisco Secure Web Appliance, sélectionnez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Realm** (Ajouter un domaine).

Étape 3 Attribuez un nom unique au domaine d'authentification en utilisant uniquement des caractères alphanumériques et des espaces.

Étape 4 Sélectionnez **Active Directory** dans le champ Authentication Protocol (Protocole d'authentification).

Étape 5 Entrez jusqu'à trois noms de domaine complets ou adresses IP pour le ou les serveurs Active Directory.

Exemple : `ntlm.exemple.com`.

Une adresse IP n'est requise que si les serveurs DNS configurés sur l'appliance ne peuvent pas résoudre le nom d'hôte du serveur Active Directory.

Si plusieurs serveurs d'authentification sont configurés dans le domaine, l'appliance tente d'autoriser jusqu'à trois serveurs d'authentification avant de ne pas autoriser la transaction dans ce domaine.

Étape 6 Joignez l'appliance au domaine :

a) Configurez le compte Active Directory :

Paramètres	Description
Active Directory Domain (Domaine Active Directory)	Nom de domaine du serveur Active Directory. Également appelé domaine ou domaine DNS.
NetBIOS domain name (Nom de domaine NETBIOS)	Si le réseau utilise NetBIOS, indiquez le nom de domaine. **Tip** Si cette option n'est pas disponible, utilisez la commande de l'interface de ligne de commande `setntlmsecuritymode` pour vérifier que le mode de sécurité NTLM est défini sur « domaine ».

Paramètres	Description
Computer Account (Compte d'ordinateur)	Indiquez un emplacement dans le domaine Active Directory où AsyncOS créera un compte d'ordinateur Active Directory, également appelé « compte approuvé d'ordinateur » pour identifier de manière unique l'ordinateur dans le domaine. Si l'environnement Active Directory supprime automatiquement des objets ordinateur à des intervalles particuliers, spécifiez un emplacement pour le compte d'ordinateur qui se trouve dans un conteneur, protégé contre la suppression automatique.
Enable Trusted Domain Lookup (Activer la recherche dans les domaines approuvés)	L'option **Enable Trusted Domain Lookup** (Activer la recherche dans les domaines approuvés) est ajoutée dans la section **Active Directory Account** [**Network** > **Authentication** > **Add Realm** (Réseau > Authentification > Ajouter un domaine)] afin de contrôler le comportement de la recherche de domaines approuvés pour le domaine. Cette option est activée par défaut.

b) Cliquez sur **Join Domain** (Joindre le domaine).

Note Si vous tentez de rejoindre un domaine que vous avez déjà rejoint (même si vous utilisez les mêmes informations d'authentification), les connexions existantes seront fermées, car Active Directory enverra un nouvel ensemble de clés à tous les clients, y compris ce Secure Web Appliance. Les clients concernés devront se déconnecter et se reconnecter.

Note Le nom d'hôte du Secure Web Appliance déployé sur AWS doit être unique. Vous devez modifier la première chaîne du nom d'hôte pour créer un nom d'hôte unique.

Par exemple, si « mgmt » est ajouté au nom d'hôte comme première chaîne, vous pouvez la modifier comme suit : « mgmt<*wsa_hostname*> ».

c) Indiquez les coordonnées de connexion (nom d'utilisateur et phrase secrète) du compte sur Active Directory, puis cliquez sur Create Account (Créer le compte).

Étape 7 (Facultatif) Configurez une identification transparente de l'utilisateur.

Paramètres	Description
Enable Transparent User Identification using Active Directory agent (Activer l'identification transparente de l'utilisateur à l'aide de l'agent Active Directory)	Entrez le nom de serveur de l'ordinateur sur laquelle l'agent principal Context Directory est installé, ainsi que le secret partagé utilisé pour y accéder. (Facultatif) Saisissez le nom de serveur de l'ordinateur sur lequel un agent Context Directory de secours est installé, ainsi que son secret partagé.

Étape 8 Configurez la sécurité du réseau :

Paramètres	Description
Client Signing Required (Signature du client requise)	Sélectionnez cette option si le serveur Active Directory est configuré pour exiger la signature du client. La sélection de cette option permet la signature SMB : • Pour placer la signature numérique lorsque l'appliance se connecte à Active Directory. • Prévenir les attaques de type homme du milieu.

Étape 9 Si vous comptez utiliser la haute disponibilité, cochez la case **Use keytab authentication** (Utiliser l'authentification keytab) dans la section Kerberos High Availability (Kerberos haute disponibilité).

a) Saisissez le nom d'utilisateur et le mot de passe.

Entrez le nom d'utilisateur Active Directory associé au(x) SPN correspondant à l'adresse IP ou au nom d'hôte de la grappe à haute disponibilité. N'incluez pas le nom de domaine dans le nom d'utilisateur (par exemple, entrez « jeanuntel » plutôt que « DOMAINE\jeanuntel » ou « jeanuntel@domaine »). Consultez Création d'un compte de service dans Windows Active Directory pour l'authentification Kerberos dans les déploiements à haute disponibilité, on page 113 pour obtenir des renseignements précis sur la création d'un compte de service qui sera utilisé pour l'authentification dans les déploiements à haute disponibilité.

b) Répétez cette étape pour tous les périphériques de la grappe à haute disponibilité.

Note Si votre appliance se trouve derrière un périphérique de répartition du trafic HTTP/HTTPS comme un équilibreur de charge, vous devez associer le SPN du périphérique de répartition du trafic dans Active Directory à un compte d'utilisateur et saisir les informations d'authentification de ce compte d'utilisateur dans la section Kerberos High Availability (Kerberos haute disponibilité). Le SPN du premier périphérique qui redirige le trafic dans la topologie du réseau doit être ajouté. Par exemple, si le trafic réseau sortant des périphériques clients passe par un gestionnaire de trafic, un équilibreur de charge, puis vers Secure Web Appliance, le SPN du gestionnaire de trafic doit être ajouté à un compte d'utilisateur sur Active Directory, et les identifiants de l'utilisateur doivent être saisis dans cette section. En effet, le gestionnaire de trafic est le premier périphérique à rencontrer le trafic des périphériques clients.

Étape 10 (Facultatif) Cliquez sur **Start Test** (Commencer le test). Vous pourrez ainsi tester les paramètres que vous avez saisis et vous assurer qu'ils sont corrects avant que les utilisateurs réels ne les utilisent pour s'authentifier. Pour en savoir plus sur les tests réalisés, consultez Utilisation de plusieurs domaines et domaines NTLM, on page 130.

Étape 11 Résolvez les problèmes détectés au cours des tests. Consultez Outils de résolution de problèmes pour les problèmes d'authentification , on page 635.

Étape 12 Envoyez et validez vos modifications.

What to do next

Créez un profil d'identification qui utilise le schéma d'authentification Kerberos. Classification des utilisateurs et logiciels clients, on page 153.

Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique)

Conditions préalables à la création d'un domaine d'authentification Active Directory (NTLMSSP et basique)

- Assurez-vous de disposer des droits et des informations de domaine nécessaires pour joindre le domaine Secure Web Appliance au domaine Active Directory auprès duquel vous souhaitez vous authentifier.
- Si vous envisagez d'utiliser « domain » comme mode de sécurité NTLM, utilisez uniquement les groupes Active Directory imbriqués. Si les groupes Active Directory ne sont pas imbriqués, utilisez la valeur par défaut, « ads ». Consultez `setntlmsecuritymode` dans la rubrique Interface de ligne de commande de ce guide.
- Comparez l'heure actuelle sur Secure Web Appliance avec l'heure actuelle du serveur Active Directory et vérifiez que la différence n'est pas supérieure à l'heure spécifiée dans l'option « Maximum tolerance for computer clock synchronization » (Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur) sur le serveur Active Directory.
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, soyez prêt à vous assurer que les domaines d'authentification du même nom sur différents Secure Web Appliance ont des propriétés identiques définies sur chaque appliance.
- Sachez qu'une fois que vous avez validé le nouveau domaine, vous ne pourrez plus modifier le protocole d'authentification de ce domaine.
- Le Secure Web Appliance doit se connecter aux contrôleurs de domaine pour tous les domaines approuvés et aux contrôleurs de domaine configurés dans le domaine NTLM. Pour que l'authentification fonctionne correctement, vous devez ouvrir les ports suivants sur tous les contrôleurs du domaine interne et du domaine externe :
  - LDAP (389 UDP et TCP)
  - Microsoft SMB (445 TCP)
  - Kerberos (88 TCP)
  - Résolution des terminaux : port fixe de mappeur de port (135 TCP) Net Log-on
- Pour NTLMSSP, la connexion unique (SSO) peut être configurée sur les navigateurs clients. Consultez Configuration de la connexion unique, on page 113.

À propos de l'utilisation de plusieurs domaines et domaines NTLM

Les règles suivantes s'appliquent à l'utilisation de plusieurs domaines et domaines NTLM :

- Vous pouvez créer jusqu'à 10 domaines d'authentification NTLM.
- Les adresses IP client d'un domaine NTLM ne doivent pas se chevaucher avec les adresses IP client d'un autre domaine NTLM.
- Chaque domaine NTLM ne peut joindre qu'un seul domaine Active Directory, mais peut authentifier les utilisateurs de tous les domaines approuvés par ce domaine. Cette approbation s'applique par défaut aux autres domaines de la même forêt et aux domaines en dehors de la forêt pour lesquels il existe au moins une approbation unidirectionnelle.

- Créez des domaines NTLM supplémentaires pour authentifier les utilisateurs dans des domaines qui ne sont pas approuvés par les domaines NTLM existants.

Création d'un domaine d'authentification Active Directory (NTLMSSP et basique)

Before you begin

Assurez-vous que les ports de la plage supérieure sur l'appliance (49152 à 65535) sont débloqués dans votre pare-feu. Ces ports sont nécessaires pour effectuer les demandes de recherche de groupe asynchrones. Le blocage de ces ports peut entraîner des défaillances intermittentes de l'authentification.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Realm** (Ajouter un domaine).

Étape 3 Attribuez un nom unique au domaine d'authentification en utilisant uniquement des caractères alphanumériques et des espaces.

Étape 4 Sélectionnez **Active Directory** dans le champ Authentication Protocol and Scheme(s) (Protocole et schéma(s) d'authentification).

Étape 5 Entrez jusqu'à trois noms de domaine complets ou adresses IP pour le ou les serveurs Active Directory.

Exemple : `active.exemple.com`.

Une adresse IP n'est requise que si les serveurs DNS configurés sur l'appliance ne peuvent pas résoudre le nom d'hôte du serveur Active Directory.

Si plusieurs serveurs d'authentification sont configurés dans le domaine, l'appliance tente d'autoriser jusqu'à trois serveurs d'authentification avant de ne pas autoriser la transaction dans ce domaine.

Étape 6 Joignez l'appliance au domaine :

a) Configurez le compte Active Directory :

Paramètres	Description
Active Directory Domain (Domaine Active Directory)	Nom de domaine du serveur Active Directory. Également appelé domaine ou domaine DNS.
NetBIOS domain name (Nom de domaine NETBIOS)	Si le réseau utilise NetBIOS, indiquez le nom de domaine.
Computer Account (Compte d'ordinateur)	Spécifiez un emplacement dans le domaine Active Directory où AsyncOS créera un compte d'ordinateur Active Directory, également appelé « compte approuvé d'ordinateur », pour identifier de manière unique l'ordinateur dans le domaine. Si l'environnement Active Directory supprime automatiquement des objets ordinateur à des intervalles particuliers, spécifiez un emplacement pour le compte d'ordinateur qui se trouve dans un conteneur, protégé contre la suppression automatique.

Paramètres	Description
Enable Trusted Domain Lookup (Activer la recherche dans les domaines approuvés)	L'option **Enable Trusted Domain Lookup** (Activer la recherche dans les domaines approuvés) est ajoutée dans la section **Active Directory Account** [**Network** > **Authentication** > **Add Realm** (Réseau > Authentification > Ajouter un domaine)] afin de contrôler le comportement de la recherche de domaines approuvés pour le domaine. Cette option est activée par défaut.

b) Cliquez sur **Join Domain** (Joindre le domaine).

Note Si vous tentez de rejoindre un domaine que vous avez déjà rejoint (même si vous utilisez les mêmes informations d'authentification), les connexions existantes seront fermées, car Active Directory enverra un nouvel ensemble de clés à tous les clients, y compris ce Secure Web Appliance. Les clients concernés devront se déconnecter et se reconnecter.

Note Le nom d'hôte du Secure Web Appliance déployé sur AWS doit être unique. Vous devez modifier la première chaîne du nom d'hôte pour créer un nom d'hôte unique.

Par exemple, si « mgmt » est ajouté au nom d'hôte comme première chaîne, vous pouvez la modifier comme suit : « mgmt<*wsa_hostname*> ».

c) Entrez le nom d'utilisateur et la phrase secrète sAMAccountName pour un utilisateur Active Directory existant qui possède des droits pour créer des comptes d'ordinateur dans le domaine.

Exemple : « `jazzdoe` » Ne pas utiliser : « `DOMAIN\jazzdoe` » ou « `jazzdoe@domain` »

Ces renseignements sont utilisés une seule fois pour établir le compte d'ordinateur et ne sont pas enregistrés.

d) Cliquez sur **Create Account** (Créer un compte).

Étape 7 (Facultatif) Configurez l'authentification transparente.

Paramètres	Description
Enable Transparent User Identification using Active Directory agent (Activer l'identification transparente de l'utilisateur à l'aide de l'agent Active Directory)	Entrez le nom de serveur de l'ordinateur sur laquelle l'agent principal Context Directory est installé, ainsi que le secret partagé utilisé pour y accéder. (Facultatif) Saisissez le nom de serveur de l'ordinateur sur lequel un agent Context Directory de secours est installé, ainsi que son secret partagé.

Étape 8 Configurez la sécurité du réseau :

Paramètres	Description
Client Signing Required (Signature du client requise)	Sélectionnez cette option si le serveur Active Directory est configuré pour exiger la signature du client. La sélection de cette option permet la signature SMB : • Pour placer la signature numérique lorsque l'appliance se connecte à Active Directory. • Prévenir les attaques de type homme du milieu.

Étape 9 (Facultatif) Cliquez sur **Start Test** (Commencer le test). Cela permettra de tester les paramètres que vous avez saisis, pour s'assurer qu'ils sont corrects avant que les utilisateurs réels ne les utilisent pour s'authentifier.

Étape 10 Envoyez et validez vos modifications.

Création d'un domaine d'authentification LDAP

Before you begin

- Obtenez les informations suivantes sur LDAP au sein de votre organisation :
  - Version LDAP
  - Adresses des serveurs
  - Ports LDAP
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, assurez-vous que les domaines d'authentification du même nom sur différents Secure Web Applianceont des propriétés identiques définies sur chaque appliance.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Realm** (Ajouter un domaine).

Étape 3 Attribuez un nom unique au domaine d'authentification en utilisant uniquement des caractères alphanumériques et des espaces.

Étape 4 Sélectionnez **LDAP** dans le champ Authentication Protocol and Scheme(s) [Protocole et schéma(s) d'authentification].

Étape 5 Saisissez les paramètres d'authentification LDAP :

Paramètres	Description
LDAP Version (Version LDAP)	Choisissez la version de LDAP et indiquez si vous souhaitez utiliser ou non le LDAP sécurisé. L'appliance prend en charge les versions 2 et 3 de LDAP. Le LDAP sécurisé nécessite la version 3 de LDAP. Indiquez si ce serveur LDAP prend en charge ou non Novell eDirectory avec une identification transparente des utilisateurs.

Paramètres	Description
LDAP Server (Serveur LDAP)	Saisissez l'adresse IP du serveur LDAP ou le nom d'hôte et son numéro de port. Vous pouvez définir jusqu'à trois serveurs. Le nom d'hôte doit être un nom de domaine complet. Par exemple, `ldap.exemple.com`. Une adresse IP est requise uniquement si les serveurs DNS configurés sur l'appliance ne peuvent pas résoudre le nom d'hôte du serveur LDAP. Le numéro de port par défaut du LDAP standard est 389. Le numéro par défaut du LDAP sécurisé est 636. Si le serveur LDAP est un serveur Active Directory, entrez le nom d'hôte ou l'adresse IP et le port du contrôleur de domaine ici. Chaque fois que cela est possible, entrez le nom du serveur de catalogue global et utilisez le port 3268. Cependant, vous pouvez souhaiter utiliser un contrôleur de domaine local lorsque le serveur de catalogue global est physiquement éloigné et que vous savez que vous n'avez qu'à authentifier les utilisateurs sur le contrôleur de domaine local. **Remarque :** Lorsque vous configurez plusieurs serveurs d'authentification dans le domaine, l'appliance tente d'autoriser jusqu'à trois serveurs d'authentification avant l'échec de l'authentification de la transaction dans ce domaine. À partir d'AsyncOS version 11.5, vous pouvez spécifier l'interface source pour LDAP/NTLM (communication avec le contrôleur de domaine). Cochez la case **Set Source Interface** (Définir l'interface source), puis sélectionnez l'interface source dans la liste déroulante.
LDAP Persistent Connections (Connexions persistantes LDAP) [sous la section Advanced (Niveau avancé)]	Choisissez l'une des valeurs suivantes : • **Use persistent connections (unlimited)** [Utiliser des connexions persistantes (illimitées)]. Use existing connections (Utiliser des connexions existantes). Si aucune connexion n'est disponible, une nouvelle connexion est ouverte. • **Use persistent connections** (Utiliser des connexions persistantes). Utilisez les connexions existantes pour traiter le nombre de requêtes spécifié. Lorsque le maximum est atteint, établissez une nouvelle connexion au serveur LDAP. • **Do not use persistent connections** (Ne pas utiliser de connexions persistantes). Créez toujours une nouvelle connexion au serveur LDAP.

Paramètres	Description
User Authentication (Authentification de l'utilisateur)	Renseignez les champs suivants : **Base Distinguished Name (Base DN)** [Nom de base distinctif (ND de base)] La base de données LDAP a une structure d'annuaire de type arborescence et l'appliance utilise le ND de base pour accéder à l'emplacement correct dans l'arborescence de l'annuaire LDAP pour commencer une recherche. Une chaîne de filtre de ND de base valide se compose d'un ou de plusieurs composants au format `objet-valeur`. Par exemple , `dc=nomsociété, dc=com`. **Note** Après la mise à niveau vers cette version, vous ne pouvez pas effectuer de test de démarrage pour l'authentification LDAP si ce champ est vide. **User Name Attribute** (Attribut de nom d'utilisateur) Choisissez l'une des valeurs suivantes : • **uid**, **cn** et **sAMAccountName.** Identifiants uniques dans l'annuaire LDAP qui spécifient un nom d'utilisateur. • **custom.** Identifiant personnalisé, tel que `UserAccount`. **User Filter Query** (Requête de filtre utilisateur) La requête de filtre utilisateur est un filtre de recherche LDAP qui localise le ND de base des utilisateurs. Cela est obligatoire si l'annuaire des utilisateurs se trouve dans une hiérarchie inférieure au ND de base ou si le nom de connexion n'est pas inclus dans le composant propre à l'utilisateur du ND de base des utilisateurs. Choisissez l'une des valeurs suivantes : • **none.** Filtre tous les utilisateurs. • **custom.** Filtre un groupe particulier d'utilisateurs.
Query Credentials (Identifiants de requête)	Indiquez si le serveur d'authentification accepte ou non les requêtes anonymes. Si le serveur d'authentification accepte les requêtes anonymes, choisissez **Server Accepts Anonymous Queries** (Le serveur accepte les requêtes anonymes). Si le serveur d'authentification n'accepte pas les requêtes anonymes, choisissez **Use Bind DN** (Utiliser le ND de liaison), puis saisissez les informations suivantes : • **Bind DN** (ND de liaison). Utilisateur sur le serveur LDAP externe autorisé à effectuer une recherche dans l'annuaire LDAP. En règle générale, le ND de liaison doit être autorisé à effectuer une recherche dans tout l'annuaire. • **Passphrase** (Phrase secrète). Phrase secrète associée à l'utilisateur que vous saisissez dans le champ Bind DN (ND de liaison). Le texte suivant répertorie des exemples d'utilisateurs pour le champ Bind DN (ND de liaison) : cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com. Si le serveur LDAP est un serveur Active Directory, vous pouvez également saisir le nom d'utilisateur du ND de liaison au format « DOMAINE\nom d'utilisateur ».

Étape 6 (Facultatif) Activez l'autorisation de groupe par le biais d'un objet de groupe ou d'un objet utilisateur et définissez les paramètres en conséquence pour l'option choisie :

Paramètre d'objet de groupe	Description
Group Membership Attribute Within Group Object (Attribut d'appartenance au groupe dans l'objet de groupe)	Choisissez l'attribut LDAP qui répertorie tous les utilisateurs appartenant à ce groupe. Choisissez l'une des valeurs suivantes : • **member** et **uniquemember.** Identifiants uniques dans l'annuaire LDAP qui désignent les membres du groupe. • **custom.** Identifiant personnalisé, tel que `UserInGroup`.
Attribute that Contains the Group Name (Attribut qui contient le nom du groupe)	Choisissez l'attribut LDAP qui désigne le nom de groupe pouvant être utilisé dans la configuration de groupe de politiques. Choisissez l'une des valeurs suivantes : • **cn.** Identifiant unique dans l'annuaire LDAP qui spécifie le nom d'un groupe. • **custom.** Identifiant personnalisé, tel que `FinanceGroup`.
Query String to Determine if Object is a Group (Chaîne de requête déterminant si l'objet est un groupe)	Choisissez un filtre de recherche LDAP qui détermine si un objet LDAP représente un groupe d'utilisateurs. Choisissez l'une des valeurs suivantes : • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.** Filtre personnalisé, tel que `objectclass=person`. **Remarque :** La requête définit l'ensemble de groupes d'authentification qui peuvent être utilisés dans les groupes de politiques.

Paramètre de l'objet utilisateur	Description
Group Membership Attribute Within User Object (Attribut de membre du groupe dans l'objet utilisateur)	Choisissez l'attribut répertoriant tous les groupes auxquels cet utilisateur appartient. Choisissez l'une des valeurs suivantes : • **memberOf.** Identifiants uniques dans l'annuaire LDAP qui désignent les membres utilisateurs. • **custom.** Identifiant personnalisé, tel que `UserInGroup`.
Group Membership Attribute is a DN (L'attribut d'appartenance au groupe est un ND)	Indiquez si l'attribut d'appartenance à un groupe est un nom distinctif (ND) qui fait référence à un objet LDAP. Activez cette option pour les serveurs Active Directory. Lorsque cette option est activée, vous devez configurer les paramètres suivants.

Paramètre de l'objet utilisateur	Description
Attribute that Contains the Group Name (Attribut qui contient le nom du groupe)	Lorsque l'attribut d'appartenance à un groupe est un ND, cela spécifie l'attribut qui peut être utilisé comme nom de groupe dans les configurations de groupe de politiques. Choisissez l'une des valeurs suivantes : • **cn.** Identifiant unique dans l'annuaire LDAP qui spécifie le nom d'un groupe. • **custom.** Identifiant personnalisé, tel que `FinanceGroup`.
Query String to Determine if Object is a Group (Chaîne de requête déterminant si l'objet est un groupe)	Choisissez un filtre de recherche LDAP qui détermine si un objet LDAP représente un groupe d'utilisateurs. Choisissez l'une des valeurs suivantes : • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.** Filtre personnalisé, tel que `objectclass=person`. **Remarque :** La requête définit l'ensemble des groupes d'authentification qui peuvent être utilisés dans les politiques Web Security Manager.

Étape 7 (Facultatif) Configurez l'authentification LDAP externe pour les utilisateurs.

a) Sélectionnez **External Authentication Queries** (Requêtes d'authentification extérieure).

b) Déterminez les comptes d'utilisateur :

Nom unique de base	ND de base permettant d'accéder à l'emplacement correct dans l'arborescence de l'annuaire LDAP pour commencer une recherche.

Query String (Chaîne de requête)	Requête permettant de renvoyer l'ensemble des groupes d'authentification, par exemple :
	`(&(objectClass=posixAccount)(uid={u}))`
	ou
	`(&(objectClass=user)(sAMAccountName={u}))`

Attribute containing the user's full name (Attribut contenant le nom complet de l'utilisateur)	Attribut LDAP, par exemple displayName ou gecos .

c) (Facultatif) Refusez la connexion aux comptes expirés en fonction des attributs LDAP d'expiration du compte RFC 2307.

d) Fournissez une requête permettant de récupérer les informations de groupe des utilisateurs.

Si un utilisateur appartient à plusieurs groupes LDAP avec des rôles utilisateur différents, AsyncOS accorde à l'utilisateur les autorisations correspondants au rôle le plus restrictif.

Nom unique de base	ND de base permettant d'accéder à l'emplacement correct dans l'arborescence de l'annuaire LDAP pour commencer une recherche.
Query String (Chaîne de requête)	`(&(objectClass=posixAccount)(uid={u}))`
Attribute containing the user's full name (Attribut contenant le nom complet de l'utilisateur)	`gecos`

Étape 8 (Facultatif) Cliquez sur **Start Test** (Commencer le test). Vous pourrez ainsi tester les paramètres que vous avez saisis et vous assurer qu'ils sont corrects avant que les utilisateurs réels ne les utilisent pour s'authentifier. Pour en savoir plus sur les tests réalisés, consultez Utilisation de plusieurs domaines et domaines NTLM, on page 130.

Note Une fois que vous avez envoyé et validé vos modifications, vous ne pourrez plus modifier le protocole d'authentification d'un domaine par la suite.

Étape 9 Envoyez et validez vos modifications.

What to do next

Créez un profil d'identification qui utilise le schéma d'authentification Kerberos. Consultez Classification des utilisateurs et logiciels clients, on page 153.

Thèmes connexes

- Authentification extérieure, on page 116

Utilisation de plusieurs domaines et domaines NTLM

Les règles suivantes s'appliquent à l'utilisation de plusieurs domaines et domaines NTLM :

- Vous pouvez créer jusqu'à 10 domaines d'authentification NTLM.
- Les adresses IP client d'un domaine NTLM ne doivent pas se chevaucher avec les adresses IP client d'un autre domaine NTLM.
- Chaque domaine NTLM ne peut joindre qu'un seul domaine Active Directory, mais peut authentifier les utilisateurs de tous les domaines approuvés par ce domaine. Cette approbation s'applique par défaut aux autres domaines de la même forêt et aux domaines en dehors de la forêt pour lesquels il existe au moins une approbation unidirectionnelle.
- Créez des domaines NTLM supplémentaires pour authentifier les utilisateurs dans des domaines qui ne sont pas approuvés par les domaines NTLM existants.

À propos de la suppression de domaines d'authentification

La suppression d'un domaine d'authentification désactive les identités associées, ce qui supprime ces identités des politiques associées.

La suppression d'un domaine d'authentification le supprime des séquences.

Configuration des paramètres d'authentification globaux

Configurez les paramètres d'authentification globaux pour appliquer des paramètres à tous les domaines d'authentification, indépendamment de leurs protocoles d'authentification.

Le mode de déploiement du proxy Web affecte les paramètres d'authentification globaux que vous pouvez configurer. Des paramètres supplémentaires sont disponibles en cas de déploiement en mode transparent par rapport au mode de transfert explicite.

Before you begin

Familiarisez-vous avec les concepts suivants :

- Échec de l'authentification, on page 141
- Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes, on page 145

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Modifiez les paramètres dans la section Global Authentication Settings (Paramètres d'authentification globaux) :

Paramètres	Description
Action if Authentication Service Unavailable (Action si le service d'authentification n'est pas disponible)	Choisissez l'une des valeurs suivantes : • **Permit traffic to proceed without authentication** (Autoriser la poursuite du trafic sans authentification). Le traitement se poursuit comme si l'utilisateur était authentifié. • **Block all traffic if user authentication fails** (Bloquer l'intégralité du trafic en cas d'échec de l'authentification de l'utilisateur). Le traitement est interrompu et l'intégralité du trafic est bloquée.
Failed Authentication Handling (Échec de la gestion de l'authentification)	Lorsque vous accordez aux utilisateurs un accès invité dans une politique de profil d'identification, ce paramètre détermine comment le proxy Web identifie et connecte l'utilisateur en tant qu'invité dans les journaux d'accès. Pour en savoir plus sur l'octroi d'un accès invité aux utilisateurs, consultez Octroi d'un accès invité après échec de l'authentification, on page 144.

Paramètres	Description
Re-authentication (Réauthentification) (Activer l'invite de réauthentification si l'utilisateur final est bloqué par la catégorie d'URL ou la restriction de session de l'utilisateur)	Ce paramètre permet aux utilisateurs de s'authentifier à nouveau si l'accès à un site Web de l'utilisateur est interdit en raison d'une politique de filtrage d'URL restrictive ou de l'interdiction de se connecter à une autre adresse IP. L'utilisateur voit une page de blocage qui comprend un lien qui lui permet d'entrer de nouveaux identifiants d'authentification. Si l'utilisateur saisit des identifiants qui permettent un accès plus étendu, la page demandée s'affiche dans le navigateur. **Remarque :** Ce paramètre s'applique uniquement aux utilisateurs authentifiés qui sont bloqués en raison de politiques de filtrage d'URL restrictives ou de restrictions de session utilisateur. Il ne s'applique pas aux transactions bloquées par sous-réseau sans authentification. Pour en savoir plus, consultez Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes, on page 145.
Basic Authentication Token TTL (Durée de vie du jeton d'authentification de base)	Contrôle la durée pendant laquelle les informations d'authentification de l'utilisateur sont stockées dans le cache avant de les revalider auprès du serveur d'authentification. Ces informations incluent le nom d'utilisateur et la phrase secrète, ainsi que les groupes d'annuaires associés à l'utilisateur. La valeur par défaut est le paramètre recommandé. Lorsque le paramètre Surrogate Timeout (Délai d'expiration de substitution) est configuré et est supérieur à la durée de vie du jeton d'authentification de base, la valeur du délai d'expiration de substitution est prioritaire et le proxy Web contacte le serveur d'authentification après l'expiration du délai de substitution.

Les autres paramètres d'authentification que vous pouvez configurer dépendent du déploiement du proxy Web, en mode de transfert transparent ou explicite.

Étape 4 Si le proxy Web est déployé en mode transparent, modifiez les paramètres comme suit :

Paramètres	Description
Credential Encryption (Chiffrement des informations d'authentification)	Ce paramètre spécifie si le client envoie ou non les coordonnées de connexion au proxy Web au moyen d'une connexion HTTPS chiffrée. Ce paramètre s'applique aux schémas d'authentification de base et NTLMSSP, mais il est particulièrement utile pour le schéma d'authentification de base, car les informations d'authentification de l'utilisateur sont envoyées en texte brut. Pour en savoir plus, consultez Échec de l'authentification, on page 141.
HTTPS Redirect Port (Port de redirection HTTPS)	Indiquez un port TCP à utiliser pour la redirection des demandes d'authentification des utilisateurs sur une connexion HTTPS. Ce paramètre spécifie le port que le client ouvrira une connexion au proxy Web à l'aide de HTTPS. Cela se produit lorsque le chiffrement des informations d'authentification est activé ou lors de l'utilisation du contrôle d'accès et que les utilisateurs sont invités à s'authentifier.

Paramètres	Description
Redirect Hostname (Nom d'hôte de redirection)	Entrez le nom d'hôte court de l'interface réseau sur laquelle le proxy Web écoute les connexions entrantes. Lorsque vous configurez l'authentification sur une appliance déployée en mode transparent, le proxy Web utilise ce nom d'hôte dans l'URL de redirection envoyée aux clients pour authentifier les utilisateurs. Vous pouvez saisir les valeurs suivantes : • **Single word hostname** (Nom d'hôte en un seul mot). Vous pouvez entrer le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Cela permet aux clients de réaliser une véritable connexion unique avec Internet Explorer sans configuration supplémentaire côté navigateur. Assurez-vous d'entrer le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Par exemple, si vos clients se trouvent dans le domaine monentreprise.com et que l'interface sur laquelle le proxy Web écoute a le nom d'hôte complet **`proxy.monentreprise.com`**, vous devez saisir **`proxy`** dans ce champ. Les clients effectuent une recherche sur le proxy et devraient être en mesure de résoudre **`proxy.monentreprise.com`**. • **Nom de domaine complet** [Nom de domaine complet (FQDN).] Vous pouvez également saisir le nom de domaine complet (FQDN) ou l'adresse IP dans ce champ. Toutefois, si vous faites cela et que vous souhaitez une véritable connexion unique pour les navigateurs Internet Explorer et Firefox, vous devez vous assurer que le nom de domaine complet (FQDN) ou l'adresse IP est ajouté à la liste des sites approuvés du client dans les navigateurs client. La valeur par défaut est le nom de domaine complet (FQDN) de l'interface M1 ou P1, selon l'interface utilisée pour le trafic du proxy.
Options du cache des informations d'authentification : Surrogate Timeout (Délai d'expiration de la substitution)	Ce paramètre indique combien de temps le proxy Web attend avant de demander à nouveau au client ses identifiants d'authentification. Jusqu'à ce que le proxy Web demande à nouveau les informations d'authentification, il utilise la valeur stockée dans la substitution (adresse IP ou témoin). Il est courant que les agents utilisateurs, tels que les navigateurs, mettent en cache les informations d'authentification afin que l'utilisateur ne soit pas invité à saisir ses informations d'authentification à chaque fois.
Options du cache des informations d'authentification : Client IP Idle Timeout (Délai d'expiration pour inactivité du client)	Lorsque l'adresse IP est utilisée comme substitution d'authentification, ce paramètre indique la durée d'attente du proxy Web avant de demander à nouveau au client des informations d'authentification lorsque le client est inactif. Si cette valeur est supérieure au délai d'expiration de substitution, ce paramètre n'a aucun effet et les clients sont invités à s'authentifier une fois le délai d'expiration de substitution atteint. Vous pourriez souhaiter utiliser ce paramètre pour réduire la vulnérabilité des utilisateurs qui quittent leur ordinateur.

Paramètres	Description
User Session Restrictions (Restrictions des sessions utilisateur)	Ce paramètre indique si les utilisateurs authentifiés sont autorisés à accéder à Internet à partir de plusieurs adresses IP simultanément. Vous pouvez souhaiter restreindre l'accès à un appareil pour empêcher les utilisateurs de partager leurs identifiants d'authentification avec des utilisateurs non autorisés. Si un utilisateur ne peut pas se connecter sur un autre appareil, une page de notification à l'utilisateur final s'affiche. Vous pouvez choisir si les utilisateurs peuvent ou non cliquer sur un bouton pour se connecter avec un nom d'utilisateur différent à l'aide du paramètre de réauthentification sur cette page. Lorsque vous activez ce paramètre, saisissez la valeur du délai d'expiration de restriction, qui détermine le temps que les utilisateurs doivent attendre avant de pouvoir se connecter à un appareil avec une adresse IP différente. La valeur du délai d'expiration de la restriction doit être supérieure à la valeur du délai d'expiration de la substitution. Vous pouvez supprimer un utilisateur en particulier ou tous les utilisateurs du cache d'authentification à l'aide de la commande de l'interface de ligne de commande `authcache`.

Paramètres	Description
Header Based Authentication (Authentification basée sur l'en-tête)	Ce paramètre vous permet de configurer le schéma d'authentification basée sur l'en-tête pour un annuaire Active Directory. Les paramètres du cache pour l'authentification basée sur l'en-tête : • Le cache d'authentification est activé par défaut. • Le délai d'expiration du cache d'authentification est identique au délai d'expiration de substitution. • Le cache stocke le nom d'utilisateur et les groupes d'utilisateurs. **Note** Effacez le cache d'authentification si vous mettez à jour la configuration du groupe d'utilisateurs. Cochez la case **Standard Header** (En-tête standard) avec ASCII comme encodage de texte et No encoding (Aucun encodage) pour Binary (Binaire) qui sont les paramètres par défaut. Cochez la case **Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies** (Utiliser les groupes dans l'en-tête X-Authenticate-Groups/en-tête personnalisé pour les politiques d'accès correspondantes) afin de prendre en compte l'en-tête des groupes entrants. Utilisez l'option **Custom Header Name** (Nom d'en-tête personnalisé) si vous souhaitez configurer les noms d'en-tête personnalisés. **Note** Si vous cochez la case **Use Groups in X-Authenticate-Groups Header/Personal Header for matching Policies** (Utiliser des groupes dans l'en-tête X-Authenticate-Groups/l'en-tête personnel pour les politiques correspondantes) et qu'aucun en-tête X-Authenticated-Groups n'est fourni, la correspondance pourrait échouer pour les politiques d'accès. Si elle n'est pas activée, les groupes extraits d'Active Directory seront mis en correspondance avec les politiques d'accès. Cochez la case **Retain Authentication Details on Egress** (Conserver les détails d'authentification à la sortie) pour conserver les en-têtes (en-têtes d'utilisateur et de groupe) à la sortie.
Advanced (Niveau avancé)	Lorsque vous utilisez le chiffrement des identifiants ou le contrôle d'accès, vous pouvez choisir si l'appliance utilise le certificat numérique et la clé livrés avec l'appliance (certificat de démonstration de l'appliance Cisco pour la sécurité du Web) ou un certificat numérique et la clé que vous chargez ici.

Étape 5 Si le proxy Web est déployé en mode de transfert explicite, modifiez les paramètres comme suit :

Paramètres	Description
Credential Encryption (Chiffrement des informations d'authentification)	Ce paramètre spécifie si le client envoie ou non les coordonnées de connexion au proxy Web au moyen d'une connexion HTTPS chiffrée. Pour activer le chiffrement des informations d'identification, choisissez « HTTPS Redirect (Secure) » [Redirection HTTPS (sécurisée)]. Lorsque vous activez le chiffrement des informations d'authentification, des champs supplémentaires apparaissent pour permettre la configuration de la redirection des clients vers le proxy Web pour l'authentification. Ce paramètre s'applique aux schémas d'authentification de base et NTLMSSP, mais il est particulièrement utile pour le schéma d'authentification de base, car les informations d'authentification de l'utilisateur sont envoyées en texte brut. Pour en savoir plus, consultez Échec de l'authentification, on page 141.
HTTPS Redirect Port (Port de redirection HTTPS)	Indiquez un port TCP à utiliser pour la redirection des demandes d'authentification des utilisateurs sur une connexion HTTPS. Ce paramètre spécifie le port que le client ouvrira une connexion au proxy Web à l'aide de HTTPS. Cela se produit lorsque le chiffrement des informations d'authentification est activé ou lors de l'utilisation du contrôle d'accès et que les utilisateurs sont invités à s'authentifier.
Redirect Hostname (Nom d'hôte de redirection)	Entrez le nom d'hôte abrégé de l'interface réseau sur laquelle le proxy Web écoute les connexions entrantes. Lorsque vous activez le mode d'authentification ci-dessus, le proxy Web utilise ce nom d'hôte dans l'URL de redirection envoyée aux clients pour authentifier les utilisateurs. Vous pouvez saisir les valeurs suivantes : • **Single word hostname** (Nom d'hôte en un seul mot). Vous pouvez saisir le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Cela permet aux clients de réaliser une véritable connexion unique avec Internet Explorer sans configuration supplémentaire côté navigateur. Assurez-vous d'entrer le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Par exemple, si vos clients se trouvent dans le domaine monentreprise.com et que l'interface sur laquelle le proxy Web écoute a le nom d'hôte complet `proxy.monentreprise.com`, vous devez saisir `proxy` dans ce champ. Les clients effectuent une recherche sur le proxy et devraient être en mesure de résoudre `proxy.monentreprise.com`. • **Nom de domaine complet** [Nom de domaine complet (FQDN).] Vous pouvez également saisir le nom de domaine complet (FQDN) ou l'adresse IP dans ce champ. Toutefois, si vous faites cela et que vous souhaitez une véritable connexion unique pour les navigateurs Internet Explorer et Firefox, vous devez vous assurer que le nom de domaine complet (FQDN) ou l'adresse IP est ajouté à la liste des sites approuvés du client dans les navigateurs client. La valeur par défaut est le nom de domaine complet (FQDN) de l'interface M1 ou P1, selon l'interface utilisée pour le trafic du proxy.

Paramètres	Description
Options du cache des informations d'authentification : Surrogate Timeout (Délai d'expiration de la substitution)	Ce paramètre indique combien de temps le proxy Web attend avant de demander à nouveau au client ses identifiants d'authentification. Jusqu'à ce que le proxy Web demande à nouveau les informations d'authentification, il utilise la valeur stockée dans la substitution (adresse IP ou témoin). Notez qu'il est courant pour les agents utilisateurs, comme les navigateurs, de mettre en cache les identifiants d'authentification afin que l'utilisateur ne soit pas invité à saisir ses identifiants à chaque fois.
Options du cache des informations d'authentification : Client IP Idle Timeout (Délai d'expiration pour inactivité du client)	Lorsque l'adresse IP est utilisée comme substitution d'authentification, ce paramètre indique la durée d'attente du proxy Web avant de demander à nouveau au client des informations d'authentification lorsque le client est inactif. Si cette valeur est supérieure au délai d'expiration de substitution, ce paramètre n'a aucun effet et les clients sont invités à s'authentifier une fois le délai d'expiration de substitution atteint. Vous pourriez souhaiter utiliser ce paramètre pour réduire la vulnérabilité des utilisateurs qui quittent leur ordinateur.
User Session Restrictions (Restrictions des sessions utilisateur)	Ce paramètre indique si les utilisateurs authentifiés sont autorisés à accéder à Internet à partir de plusieurs adresses IP simultanément. Vous pouvez souhaiter restreindre l'accès à un appareil pour empêcher les utilisateurs de partager leurs identifiants d'authentification avec des utilisateurs non autorisés. Lorsqu'un utilisateur ne peut pas se connecter sur un autre appareil, une page de notification à l'utilisateur final s'affiche. Vous pouvez choisir si les utilisateurs peuvent ou non cliquer sur un bouton pour se connecter avec un nom d'utilisateur différent à l'aide du paramètre de réauthentification sur cette page. Lorsque vous activez ce paramètre, saisissez la valeur du délai d'expiration de restriction, qui détermine le temps que les utilisateurs doivent attendre avant de pouvoir se connecter à un appareil avec une adresse IP différente. La valeur du délai d'expiration de la restriction doit être supérieure à la valeur du délai d'expiration de la substitution. Vous pouvez supprimer un utilisateur en particulier ou tous les utilisateurs du cache d'authentification à l'aide de la commande de l'interface de ligne de commande `authcache`.

Paramètres	Description
Header Based Authentication (Authentification basée sur l'en-tête)	Ce paramètre vous permet de configurer le schéma d'authentification basée sur l'en-tête pour un annuaire Active Directory. Les paramètres du cache pour l'authentification basée sur l'en-tête : • Le cache d'authentification est activé par défaut. • Le délai d'expiration du cache d'authentification est identique au délai d'expiration de substitution. • Le cache stocke le nom d'utilisateur et les groupes d'utilisateurs. **Note** Effacez le cache d'authentification si vous mettez à jour la configuration du groupe d'utilisateurs. Cochez la case **Standard Header** (En-tête standard) avec ASCII comme encodage de texte et No encoding (Aucun encodage) pour Binary (Binaire) qui sont les paramètres par défaut. Cochez la case **Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies** (Utiliser les groupes dans l'en-tête X-Authenticate-Groups/en-tête personnalisé pour les politiques d'accès correspondantes) afin de prendre en compte l'en-tête des groupes entrants. Utilisez l'option **Custom Header Name** (Nom d'en-tête personnalisé) si vous souhaitez configurer les noms d'en-tête personnalisés. **Note** Si vous cochez la case **Use Groups in X-Authenticate-Groups Header/Personal Header for matching Policies** (Utiliser des groupes dans l'en-tête X-Authenticate-Groups/l'en-tête personnel pour les politiques correspondantes) et qu'aucun en-tête X-Authenticated-Groups n'est fourni, la correspondance pourrait échouer pour les politiques d'accès. Si elle n'est pas activée, les groupes extraits d'Active Directory seront mis en correspondance avec les politiques d'accès. Cochez la case **Retain Authentication Details on Egress** (Conserver les détails d'authentification à la sortie) pour conserver les en-têtes (en-têtes d'utilisateur et de groupe) à la sortie.
Advanced (Niveau avancé)	Lorsque vous utilisez le chiffrement des identifiants ou le contrôle d'accès, vous pouvez choisir si l'appliance utilise le certificat numérique et la clé livrés avec l'appliance (certificat de démonstration de l'appliance Cisco pour la sécurité du Web) ou un certificat numérique et la clé que vous chargez ici. Pour charger un certificat numérique et une clé, cliquez sur **Browse** (Parcourir) et accédez au fichier nécessaire sur votre ordinateur local. Cliquez ensuite sur **Upload Files** (Charger des fichiers) après avoir sélectionné les fichiers souhaités.

Étape 6 Envoyez et validez vos modifications.

Séquences d'authentification

À propos des séquences d'authentification

Utilisez des séquences d'authentification pour permettre l'authentification des utilisateurs avec des identités uniques au moyen de différents serveurs ou protocoles d'authentification. Les séquences d'authentification sont également utiles pour fournir des options de secours au cas où les options d'authentification principales étaient indisponibles.

Les séquences d'authentification sont des ensembles composés d'au moins deux domaines d'authentification. Les domaines utilisés peuvent avoir différents serveurs d'authentification et différents protocoles d'authentification. Pour en savoir plus sur les domaines d'authentification, consultez Domaines d'authentification, on page 115.

Une fois que vous avez créé un deuxième domaine d'authentification, l'appliance affiche automatiquement une section Realm Sequences (Séquences de domaines) sous Network > Authentication (Réseau > Authentification) et inclut une séquence d'authentification par défaut nommée All Realms (Tous les domaines). La séquence All Realms (Tous les domaines) comprend automatiquement chaque domaine que vous définissez. Vous pouvez modifier l'ordre des domaines dans la séquence All Realms (Tous les domaines), mais vous ne pouvez pas supprimer la séquence All Realms (Tous les domaines) ni en supprimer le moindre domaine.

Si plusieurs domaines d'authentification NTLM sont définis, Secure Web Appliance utilise le schéma d'authentification NTLMSSP avec un seul domaine d'authentification NTLM par séquence. Vous pouvez choisir le domaine d'authentification NTLM à utiliser pour NTLMSSP dans chaque séquence, notamment la séquence All Realms (Tous les domaines). Pour utiliser NTLMSSP avec plusieurs domaines NTLM, configurez un seul profil d'identification pour deux domaines d'authentification en veillant à ce qu'une seule identité soit utilisée pour All Realms (Tous les domaines). Les domaines doivent entretenir une confiance mutuelle.

Les domaines d'authentification utilisés lors de l'authentification dans une séquence dépendent des éléments suivants :

- Le schéma d'authentification utilisé. Cela est généralement dicté par le type d'informations d'authentification saisies sur le client.
- L'ordre dans lequel les domaines sont répertoriés dans la séquence (pour les domaines Basic (De base) uniquement, car un seul domaine NTLMSSP est possible).

Tip Pour des performances optimales, authentifiez les clients sur le même sous-réseau à l'aide d'un seul domaine.

Création de séquences d'authentification

Before you begin

- Créez deux domaines d'authentification ou plus (voir Domaines d'authentification, on page 115).
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, assurez-vous que les domaines d'authentification du même nom sur différents Secure Web Applianceont des propriétés identiques définies sur chaque appliance.
- Sachez qu'AsyncOS utilisera les domaines pour traiter l'authentification de manière successive, en commençant par le premier domaine de la liste.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Sequence** (Ajouter une séquence).

Étape 3 Saisissez un nom unique pour la séquence en utilisant des caractères alphanumériques et des espaces.

Étape 4 Dans la première ligne de la zone Realm Sequence for Basic System (Séquence de domaine pour le schéma de base), choisissez le premier domaine d'authentification que vous souhaitez inclure dans la séquence.

Étape 5 Dans la deuxième ligne de la zone Realm Sequence for Basic System (Séquence de domaine pour le schéma de base), choisissez le domaine suivant à inclure dans la séquence.

Étape 6 (Facultatif) Cliquez sur **Add Row** (Ajouter une ligne) pour inclure un autre domaine qui utilise les informations d'authentification de base.

Étape 7 Si un domaine NTLM est défini, choisissez-en un dans le champ Realm (Domaine) pour le schéma NTLMSSP.

Le proxy Web utilise ce domaine NTLM lorsque le client envoie les informations d'authentification NTLMSSP.

Étape 8 Envoyez et validez vos modifications.

Modification et réorganisation des séquences d'authentification

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur le nom de la séquence que vous souhaitez modifier ou réorganiser.

Étape 3 Choisissez un nom de domaine dans la liste déroulante Realms (Domaines) sur la ligne correspondant au numéro de position que vous souhaitez que le domaine occupe dans la séquence.

Note Pour la séquence All Realms (Tous les domaines), vous pouvez uniquement modifier l'ordre de ses domaines, vous ne pouvez pas modifier les domaines eux-mêmes. Pour modifier l'ordre des domaines dans la séquence All Realms (Tous les domaines), cliquez sur les flèches dans la colonne Order (Organiser) pour repositionner les domaines correspondants.

Étape 4 Répétez l'**étape 3** jusqu'à ce que tous les domaines soient répertoriés et organisés comme requis, en vous assurant que chaque nom de domaine s'affiche sur une seule ligne.

Étape 5 Envoyez et validez vos modifications.

Suppression de séquences d'authentification

Before you begin

Sachez que la suppression d'une séquence d'authentification désactive également les identités associées, qui à leur tour suppriment ces identités des politiques associées.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur l'icône de corbeille en regard du nom de la séquence.

Étape 3 Cliquez sur **Delete** (Supprimer) pour confirmer la suppression de la séquence.

Étape 4 Validez vos modifications.

Échec de l'authentification

À propos de l'échec de l'authentification

L'accès au Web des utilisateurs peut être bloqué en raison d'un échec d'authentification pour les raisons suivantes :

- **Limites du client/agent utilisateur.** Certaines applications clientes peuvent ne pas prendre en charge correctement l'authentification. Vous pouvez contourner l'authentification pour ces clients en configurant des profils d'identification qui ne nécessitent pas d'autorisation et en fondant leurs critères sur les clients (et, éventuellement, sur les URL auxquels ils doivent accéder).
- **Le service d'authentification n'est pas disponible.** Un service d'authentification peut ne pas être disponible en raison de problèmes de réseau ou de serveur. Vous pouvez choisir d'autoriser le trafic non authentifié dans ces circonstances.
- **informations d'authentification non valides.** Certains utilisateurs peuvent ne pas être en mesure de fournir des identifiants valides pour une authentification correcte (par exemple, les visiteurs ou les utilisateurs en attente d'identifiants). Vous pouvez choisir d'accorder à ces utilisateurs un accès limité à Internet.

Thèmes connexes

- Contournement de l'authentification avec des agents utilisateur problématiques , on page 142
- Contournement de l'authentification, on page 143
- Autorisation du trafic non authentifié lorsque le service d'authentification n'est pas disponible, on page 144

• Octroi d'un accès invité après échec de l'authentification, on page 144

Contournementdel'authentificationavecdesagentsutilisateurproblématiques

Certains agents utilisateur sont connus pour avoir des problèmes d'authentification qui peuvent avoir une incidence sur leurs opérations normales.

Vous devez contourner l'authentification par les agents utilisateur suivants :

- Windows-Update-Agent
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient
- Akamai NetSession Interface
- Microsoft-CryptoAPI
- NCSI
- MSDW
- Gnotify
- msde
- Mise à jour Google

Note Les politiques d'accès continuent de filtrer (en fonction des catégories d'URL) et d'analyser le trafic (McAfee, Webroot) selon la configuration des politiques d'accès.

Étape 1 Configurez le profil d'identification pour contourner l'authentification avec les agents utilisateur indiqués :

a) Sélectionnez **Web Security Manager > Identification Profile** (Web Security Manager > Profil d'identification).
b) Cliquez sur **Add Identification Profile** (Ajouter un profil d'identification).
c) Saisissez les informations :

Option	Valeur
Name (Nom)	User Agent AuthExempt Identification Profile (Profil d'identification Authexempt d'agent utilisateur)
Insert Above (Insérer au-dessus)	Définir sur le premier profil dans l'ordre de traitement
Define Members by Subnet (Définir les membres par sous-réseau)	Laissez le champ vide.
Define Members by Authentication (Définir les membres par authentification)	Aucune authentication requise.

d) Cliquez sur **Advanced > User Agents** (Avancé > Agents utilisateur).
e) Cliquez sur **None Selected** (Aucune sélection).
f) Sous Custom user Agents (Agents utilisateur personnalisés), indiquez les chaînes d'agents utilisateur problématiques.

Étape 2 Configurez la politique d'accès :

a) Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).
b) Cliquez sur **Add Policy** (Ajouter une politique).
c) Saisissez les informations :

Option	Valeur
Policy Name (nom de la politique)	Auth Exemption for User Agents (Dispense d'autorisation pour les agents utilisateur)
Insert Above Policy (Insérer au-dessus de la politique)	Définissez la première politique dans l'ordre de traitement.
Identification Profile Policy (Politique de profil d'identification)	User Agent AuthExempt Identification Profile (Profil d'identification Authexempt d'agent utilisateur)
Advanced (Niveau avancé)	Aucun

Étape 3 Envoyez et validez vos modifications.

Contournement de l'authentification

	Étape	Autres renseignements
1	Créez une catégorie d'URL personnalisée qui contient les sites Web concernés en configurant les propriétés avancées.	Création et modification de catégories d'URL personnalisées, on page 211
2	Créez un profil d'identification ayant les caractéristiques suivantes : • Placé au-dessus de toutes les identités nécessitant une authentification. • Comprend la catégorie d'URL personnalisée. • Comprend les applications clientes concernées. • Ne requiert pas d'authentification.	Classification des utilisateurs et logiciels clients, on page 153
3	Créez une politique pour le profil d'identification.	Création d'une politique , on page 253

Thèmes connexes

- Contourner le proxy Web

Autorisation du trafic non authentifié lorsque le service d'authentification n'est pas disponible

Note Cette configuration s'applique uniquement lorsqu'un service d'authentification n'est pas disponible. Elle ne contournera pas l'authentification de façon permanente. Pour d'autres options, consultez À propos de l'échec de l'authentification, on page 141

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cliquez sur **Permit Traffic To Proceed Without Authentication** (Permettre au trafic de poursuivre sans authentification) dans le champ Action If Authentication Service Unavailable (Action en cas d'indisponibilité du service d'authentification).

Étape 4 Envoyez et validez vos modifications.

Octroi d'un accès invité après échec de l'authentification

Pour accorder l'accès invité, vous devez exécuter les procédures suivantes :

1. Définir un profil d'identification qui prend en charge l'accès invité, on page 144
2. Utiliser un profil d'identification qui prend en charge l'accès invité dans une politique, on page 145
3. (Facultatif) Configurer la façon dont les détails de l'utilisateur invité sont journalisés, on page 145

Note Si un profil d'identification permet l'accès invité et qu'aucune politique définie par l'utilisateur n'utilise ce profil d'identification, les utilisateurs qui échouent à l'authentification correspondent à la politique globale du type de politique applicable. Par exemple, si MyIdentificationProfile permet l'accès en tant qu'invité et qu'aucune politique d'accès définie par l'utilisateur n'utilise MyIdentificationProfile, les utilisateurs qui échouent à l'authentification correspondent à la politique d'accès globale. Si vous ne souhaitez pas que les utilisateurs invités correspondent à une politique globale, créez une politique supérieure à la politique globale qui s'applique aux utilisateurs invités et bloque tous les accès.

Définir un profil d'identification qui prend en charge l'accès invité

Étape 1 Choisissez **Web Security Manager > Identification Profiles** (Web Security Manager > Profils d'identification).

Étape 2 Cliquez sur **Add Identification Profile** (Ajouter un profil d'identification) pour ajouter une nouvelle identité, ou cliquez sur le nom de l'identité existante que vous souhaitez utiliser.

Étape 3 Cochez la case **Support Guest Privileges** (Prise en charge des privilèges invité).

Étape 4 Envoyez et validez vos modifications.

Utiliser un profil d'identification qui prend en charge l'accès invité dans une politique

Étape 1 Choisissez un type de politique dans le menu Web Security Manager.

Étape 2 Cliquez sur un nom de politique dans le tableau des politiques.

Étape 3 Choisissez **Select One Or More Identification Profiles** (Sélectionner un ou plusieurs profils d'identification) dans la liste déroulante Identification Profiles And Users (Profils d'identification et utilisateurs) (si ce n'est déjà fait).

Étape 4 Choisissez un **profil** qui prend en charge l'accès invité dans la liste déroulante de la colonne Identification Profile (Profil d'identification).

Étape 5 Cliquez sur le bouton radio **Guest (Users Failing Authentication)** [Invités (Utilisateurs dont l'authentification a échoué)].

Note Si cette option n'est pas disponible, cela signifie que le **profil** que vous avez choisi n'est pas configuré pour prendre en charge l'accès invité. Revenez à l'étape 4 et choisissez-en un autre, ou consultez Définir un profil d'identification qui prend en charge l'accès invité, on page 144 pour en définir un nouveau.

Étape 6 Envoyez et validez vos modifications.

Configurer la façon dont les détails de l'utilisateur invité sont journalisés

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cliquez sur un bouton radio Log Guest User By (Consigner l'utilisateur invité par), décrit ci-dessous, dans le champ Failed Authentication Handling (Échec de la gestion de l'authentification).

Bouton radio	Description
IP Address (Adresse IP)	L'adresse IP du client de l'utilisateur invité est consignée dans les journaux d'accès.
User Name As Entered By End-User (Nom d'utilisateur tel qu'il a été saisi par l'utilisateur final)	Le nom d'utilisateur dont l'authentification a initialement échoué est consigné dans les journaux d'accès.

Étape 4 Envoyez et validez vos modifications.

Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes

À propos de l'autorisation de réauthentification avec des informations d'authentification différentes

Utilisez la nouvelle authentification pour permettre aux utilisateurs de s'authentifier à nouveau, en utilisant des informations d'authentification différentes, si les informations d'authentification qu'ils ont précédemment utilisées ont échoué à l'autorisation. Un utilisateur peut s'authentifier avec succès, mais ne pas pouvoir accéder à une ressource Web s'il n'est pas autorisé à le faire. En effet, l'authentification identifie simplement les utilisateurs dans le but de transmettre leurs informations d'authentification vérifiées aux politiques, mais ce sont les politiques qui autorisent ou non ces utilisateurs à accéder aux ressources.

Un utilisateur doit s'être authentifié avec succès pour être autorisé à s'authentifier de nouveau.

- Pour utiliser la fonctionnalité de réauthentification avec les pages de notification à l'utilisateur final définies par l'utilisateur, le script CGI qui analyse l'URL de redirection doit analyser et utiliser le paramètre Reauth_URL.

Autorisation de réauthentification avec des informations d'authentification différentes

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cochez la case **Re-Authentication Prompt If End User Blocked by URL Category Or User Session Restriction** (Invite de réauthentification si l'utilisateur final est bloqué par la catégorie d'URL ou la restriction de session de l'utilisateur).

Étape 4 Cliquez sur **Submit** (Soumettre).

Suivi des utilisateurs identifiés

Note Lorsque l'appliance est configurée pour utiliser des substitutions d'authentification basées sur les témoins, elle ne reçoit pas les informations sur les témoins des clients pour les demandes HTTPS et FTP sur HTTP. Par conséquent, elle ne peut pas obtenir le nom d'utilisateur à partir du témoin.

Substituts d'authentification pris en charge pour les demandes explicites

Types de substitution	Chiffrement des informations d'authentification désactivé			Chiffrement des informations d'authentification activé		
Protocole :	HTTP	HTTPS et FTP sur HTTP	FTP natif	HTTP	HTTPS et FTP sur HTTP	FTP natif
Aucun modèle de substitution	Oui	Oui	Oui	S.O.	S.O.	S.O.
Basé sur IP	Oui	Oui	Oui	Oui	Oui	Oui
Basés sur les témoins	Oui	Oui***	Oui***	Oui	Non/Oui**	Oui***

Substituts d'authentification pris en charge pour les demandes transparentes

Note Consultez également la description des options de substitution d'authentification dans Classification des utilisateurs et logiciels clients, on page 153.

Types de substitution	Chiffrement des informations d'authentification désactivé			Chiffrement des informations d'authentification activé		
Protocole :	HTTP	HTTPS	FTP natif	HTTP	HTTPS	FTP natif
Aucun modèle de substitution	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
Basé sur IP	Oui	Non/Oui*	Non/Oui*	Oui	Non/Oui*	Non/Oui*
Basés sur les témoins	Oui	Non/Oui**	Non/Oui**	Oui	Non/Oui**	Non/Oui**

* Fonctionne après que le client a envoyé une demande à un site HTTP et qu'il est authentifié. Avant que cela ne se produise, le comportement dépend du type de transaction :

- **Transactions FTP natives.** Contournement de l'authentification des transactions.
- **Transactions HTTPS.** Les transactions sont abandonnées. Cependant, vous pouvez configurer le proxy HTTPS pour déchiffrer la première requête HTTPS à des fins d'authentification.

** Lorsque l'authentification basée sur les témoins est utilisée, le proxy Web ne peut pas authentifier l'utilisateur pour les transactions HTTPS, FTP natif et FTP sur HTTP. En raison de cette limitation, toutes les demandes HTTPS, FTP natives et FTP sur HTTP contournent l'authentification, donc l'authentification n'est pas demandée du tout.

*** Aucune substitution n'est utilisée dans ce cas, même si la substitution basée sur les témoins est configurée.

Thèmes connexes

- Profils d'identification et authentification , on page 162

Suivi des utilisateurs réauthentifiés

Avec la réauthentification, si un utilisateur plus privilégié s'authentifie et est autorisé, le proxy Web met en cache l'identité de cet utilisateur pendant différentes durées selon les substitutions d'authentification configurées :

- **Session cookie** (Témoin de session). L'identité de l'utilisateur privilégié est utilisée jusqu'à ce que le navigateur soit fermé ou que la session expire.
- **Persistent cookie** (Témoin persistant). L'identité de l'utilisateur privilégié est utilisée jusqu'à ce que la substitution expire.
- **IP address** (Adresse IP). L'identité de l'utilisateur privilégié est utilisée jusqu'à ce que la substitution expire.

- **No surrogate** (Aucune substitution). Par défaut, le proxy Web demande l'authentification à chaque nouvelle connexion, mais lorsque la réauthentification est activée, le proxy Web demande l'authentification à chaque nouvelle demande, ce qui entraîne une charge accrue du serveur d'authentification lors de l'utilisation de NTLMSSP. Cependant, il est possible que l'augmentation de l'activité d'authentification ne soit pas visible pour un utilisateur, car la plupart des navigateurs mettent en cache les informations d'authentification de l'utilisateur privilégié et s'authentifient sans invite jusqu'à la fermeture du navigateur. En outre, lorsque le proxy Web est déployé en mode transparent et que l'option « Apply same surrogate settings to explicit forward requests » (Appliquer les mêmes paramètres de substitution aux demandes de transfert explicites) n'est pas activée, aucune substitution d'authentification n'est utilisée pour les demandes de transfert explicites et la réauthentification se produira.

Note Si Secure Web Appliance utilise des témoins pour les substitutions d'authentification, Cisco recommande d'activer le chiffrement des identifiants.

Informations d'authentification

Les informations d'authentification des utilisateurs peuvent être obtenues auprès des utilisateurs en étant invités à les saisir dans leur navigateur ou dans une autre application cliente, ou en obtenant les identifiants de manière transparente d'une autre source.

Suivi des informations d'authentification pour leur réutilisation au cours d'une session

Grâce aux substitutions d'authentification, après l'authentification d'un utilisateur au cours d'une session, vous pouvez suivre les informations d'authentification en vue de les réutiliser tout au long de la session plutôt que de demander à l'utilisateur de s'authentifier à chaque nouvelle demande. Les substitutions d'authentification peuvent être basées sur l'adresse IP du poste de travail de l'utilisateur ou sur un témoin affecté à la session.

Pour Internet Explorer, assurez-vous que le nom d'hôte de redirection est le nom d'hôte court (ne contenant pas de points) ou le nom NetBIOS plutôt qu'un domaine qualifié complet. Vous pouvez également ajouter le nom d'hôte de l'appliance à la zone intranet local d'Internet Explorer [Tools > Internet options > Security tab (Outils > options Internet > onglet Sécurité)]. Cependant, cela sera requis sur chaque client. Pour plus d'informations à ce sujet, consultez Comment puis-je configurer correctement NTLM avec SSO (les informations d'authentification envoyées de manière transparente)?

Avec les navigateurs Firefox et d'autres navigateurs autres que Microsoft, les paramètres **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** et **network.automatic-ntlm-auth.trusted-uris** doivent être définis sur le nom d'hôte de redirection en mode transparent. Vous pouvez également vous reporter à Firefox n'envoie pas les informations d'authentification de manière transparente (SSO). Cet article fournit des informations générales sur la modification des paramètres de Firefox.

Pour en savoir plus sur le nom d'hôte de redirection, consultez Configuration des paramètres d'authentification globaux, on page 131 ou la commande d'interface de ligne de commande `sethostname`.

Échecs d'authentification et d'autorisation

Si l'authentification échoue pour des raisons acceptées, comme des applications client incompatibles, vous pouvez accorder l'accès en tant qu'invité.

Si l'authentification réussit, mais que l'autorisation échoue, il est possible d'autoriser la nouvelle authentification en utilisant un autre ensemble d'identifiants qui peuvent être autorisés à accéder à la ressource demandée.

Thèmes connexes

- Octroi d'un accès invité après échec de l'authentification, on page 144
- Autorisation de réauthentification avec des informations d'authentification différentes, on page 146

Format des informations d'authentification

Schéma d'authentification	Format des informations d'authentification
NTLMSSP	**`MonDomaine\jdupont`**
Basic (niveau de base)	**`jdupont`** **`MonDomaine\jdupont`** **Note** Si l'utilisateur ne saisit pas le domaine Windows, le proxy Web ajoute le domaine Windows par défaut au début.

Chiffrement des informations d'authentification pour l'authentification de base

À propos du chiffrement des informations d'authentification pour l'authentification de base

Activez le chiffrement des informations d'identification pour transmettre les informations d'authentification sur HTTPS sous forme chiffrée. Cela augmente la sécurité du processus d'authentification de base.

Le Secure Web Appliance utilise ses propres certificat et clé privée par défaut pour créer une connexion HTTPS avec le client à des fins d'authentification sécurisée. La plupart des navigateurs avertissent cependant les utilisateurs que ce certificat n'est pas valide. Pour empêcher les utilisateurs de voir le message de certificat non valide, vous pouvez télécharger un certificat valide et une paire de clés que votre organisation utilise.

Configuration du chiffrement des informations d'authentification

Before you begin

- Configurez l'appliance pour utiliser les substitutions d'adresses IP.
- (Facultatif) Obtenez un certificat et une clé privée non chiffrée. Le certificat et la clé configurés ici sont également utilisés par le contrôle d'accès.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cochez la case **Use Encrypted HTTPS Connection For Authentication** (Utiliser la connexion HTTPS chiffrée pour l'authentification) dans le champ Credential Encryption (Chiffrement des informations d'authentification).

Étape 4 (Facultatif) Modifiez le numéro de port par défaut (443) dans le champ HTTPS Redirect Port (Port de redirection HTTPS) pour les connexions HTTP du client lors de l'authentification.

Étape 5 (Facultatif) Charger le certificat et la clé :

a) Développez la section Advanced (Niveau avancé).

b) Cliquez sur **Browse** (Parcourir) dans le champ Certificat (Certificate) et trouvez le fichier de certificat que vous souhaitez télécharger.

c) Cliquez sur **Browse** (Parcourir) dans le champ Key (Clé) et trouvez le fichier de clé privée que vous souhaitez télécharger.

d) Cliquez sur **Upload Files** (Charger des fichiers).

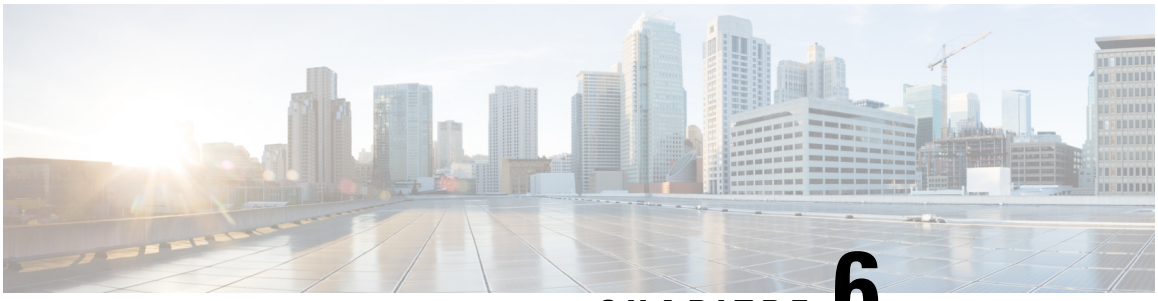
Étape 6 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Certificate Management, on page 608.

Résolution de problèmes liés à l'authentification



CHAPITRE 6

Classifier les utilisateurs finaux pour l'application des politiques

Cette rubrique contient les sections suivantes :

Survol de la classification des utilisateurs et logiciels clients

Les profils d'identification vous permettent de classer les utilisateurs et les agents utilisateurs (logiciel client) aux fins suivantes :

- Demandes de transaction groupées pour l'application des politiques (sauf les logiciels-services)
- Spécification des exigences d'identification et d'authentification

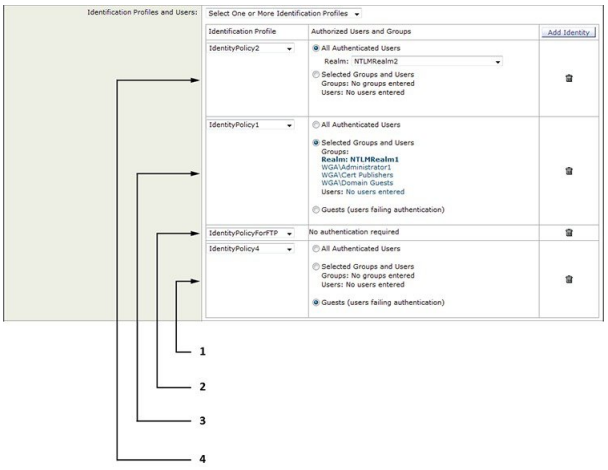
AsyncOS attribue un profil d'identification à chaque transaction :

- Profils d'identification personnalisés – AsyncOS attribue un profil personnalisé en fonction des critères de cette identité.
- Profil d'identification global – AsyncOS attribue le profil global aux transactions qui ne répondent aux critères d'aucun profil personnalisé. Par défaut, le profil global ne nécessite pas d'authentification.

AsyncOS traite les profils d'identification de manière séquence, en commençant par le premier. Le profil global est le dernier profil.

Un profil d'identification ne peut comprendre qu'un seul critère. Par ailleurs, les profils d'identification qui comprennent plusieurs critères exigent que tous les critères soient satisfaits.

Une politique peut faire appel à plusieurs profils d'identification :



1	Ce profil d'identification permet l'accès en tant qu'invité et s'applique aux utilisateurs dont l'authentification échoue.
2	L'authentification n'est pas utilisée pour ce profil d'identification.
3	Les groupes d'utilisateurs précisés dans ce profil d'identification sont autorisés pour cette politique.
4	Ce profil d'identification utilise une séquence d'authentification et cette politique s'applique à un domaine dans la séquence.

Classification des utilisateurs et des logiciels clients : bonnes pratiques

- Créez des profils d'identification moins nombreux et plus généraux qui s'appliquent à tous les utilisateurs ou à des groupes d'utilisateurs moins nombreux et plus importants. Utilisez des politiques plutôt que des profils pour une gestion plus granulaire.
- Créez des profils d'identification avec des critères uniques.
- S'il est déployé en mode transparent, créez un profil d'identification pour les sites qui ne prennent pas en charge l'authentification. Consultez Contournement de l'authentification, on page 143.

Critères du profil d'identification

Ces caractéristiques de transaction sont disponibles pour définir un profil d'identification :

Option	Description
Subnet (Sous-réseau)	Le sous-réseau client doit correspondre à la liste des sous-réseaux dans une politique.
Protocole	Le protocole utilisé dans la transaction : HTTP, HTTPS, SOCKS ou FTP natif.

Option	Description
Port	Le port proxy de la demande doit se trouver dans la liste de ports du profil d'identification, le cas échéant. Pour les connexions de transfert explicite, il s'agit du port configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination.
User Agent (Agent d'utilisateur)	L'agent utilisateur (application client) effectuant la demande doit figurer dans la liste des agents utilisateurs du profil d'identification, le cas échéant. Certains agents utilisateurs ne peuvent pas gérer l'authentification. Par conséquent, la création d'un profil qui n'exige pas d'authentification est nécessaire. Les agents utilisateurs comprennent des programmes comme les programmes de mise à jour et les navigateurs comme Internet Explorer et Mozilla Firefox.
URL Category (Catégorie URL)	La catégorie de l'URL de la demande doit faire partie de la liste des catégories d'URL du profil d'identification, le cas échéant.
Authentication requirements (Exigences relatives à l'authentification)	Si le profil d'identification nécessite une authentification, les justificatifs d'authentification du client doivent correspondre aux exigences d'authentification du profil d'identification.

Classification des utilisateurs et logiciels clients

Avant de commencer

- Créez des domaines d'authentification. Reportez-vous aux sections Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique), à la page 122 ou Création d'un domaine d'authentification LDAP, à la page 125.
- Sachez que lorsque vous validez des modifications aux profils d'identification, les utilisateurs finaux doivent s'authentifier de nouveau.
- Si vous êtes en mode Cloud Connector, sachez qu'une option supplémentaire de profil d'identification est offerte : l'ID de l'ordinateur. Consultez Identification des ordinateurs pour l'application des politiques, à la page 68.
- (Facultatif) Créez des séquences d'authentification. Voir la section Création de séquences d'authentification, à la page 140.
- (Facultatif) Activez Secure Mobility si le profil d'identification doit inclure des utilisateurs mobiles.
- (Facultatif) Découvrez les méthodes de substitution d'authentification. Voir Suivi des utilisateurs identifiés, à la page 146 .

Étape 1 Choisissez **Web Security Manager** > **Identification Profiles** (Web Security Manager > Profils d'identification).

Étape 2 Cliquez sur **Add Profile** (Ajouter un profil) pour ajouter un profil.

Étape 3 Cochez la case **Enable Identification Profile** (Activer le profil d'identification) pour activer ce profil ou pour le désactiver rapidement sans le supprimer.

Étape 4 Attribuez un **nom** de profil unique.

Étape 5 La **description** est facultative.

Étape 6 Dans la liste déroulante **Insert Above** (Insérer au-dessus), choisissez l'endroit où ce profil doit apparaître dans le tableau.

Remarque Parmi les profils d'identification de poste qui ne nécessitent pas d'authentification figurent le premier profil d'identification qui nécessite une authentification.

Étape 7 Dans la section **User Identification Method** (Méthode d'identification de l'utilisateur), choisissez une méthode d'identification, puis définissez les paramètres connexes; les options affichées varient selon la méthode choisie.

a) Choisissez une méthode d'identification dans la liste déroulante **User Identification Method** (Méthode d'identification de l'utilisateur).

Option	Description
Exempt from authentication/ identification (Dispenser d'authentification et d'identification)	Les utilisateurs sont principalement identifiés par leur adresse IP. Aucun paramètre supplémentaire n'est requis.
Authenticate users (Authentifier les utilisateurs)	Les utilisateurs sont identifiés par les justificatifs d'authentification qu'ils ont saisis.
Transparently identify users with ISE (Identification transparente des utilisateurs avec ISE)	Disponible lorsque le service ISE est activé(Network > Identity Services Engine) (Réseau > Moteur ISE). Pour ces transactions, le nom d'utilisateur et les étiquettes Groupe sécurisé associées seront obtenus à partir du moteur ISE. Dans les déploiements ISE-PIC, les informations sur les groupes et les utilisateurs ISE sont reçues. Pour en savoir plus, consultez Tâches relatives à l'intégration du service ISE/ISE-PIC, à la page 177.
Transparently identify users with authentication realm (Identification transparente des utilisateurs à l'aide du domaine d'authentification)	Cette option est disponible si un ou plusieurs domaines d'authentification sont configurés pour prendre en charge l'identification transparente.

Remarque Lorsqu'au moins un profil d'identification avec authentification ou identification transparente est configuré, les tableaux de politiques prennent en charge la définition de l'appartenance à la politique à l'aide de noms d'utilisateur, de groupes de répertoires et d'étiquettes Groupe sécurisé.

Remarque L'agent CDA (Context Directory Agent) n'est plus pris en charge. Il est recommandé de configurer ISE/ISE-PIC pour une identification transparente de l'utilisateur afin d'obtenir la même fonctionnalité.

Les options de configuration de CDA ne seront plus disponibles dans les versions ultérieures.

Pour en savoir plus, consultez https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/bulletin-c25-2428601.html.

b) Fournissez les paramètres appropriés à la méthode choisie. Les sections décrites dans ce tableau ne sont pas toutes visibles pour chaque choix.

Option de rechange au domaine d'authentification ou aux privilèges invité	Si l'authentification de l'utilisateur n'est pas disponible dans ISE : • **Support Guest Privileges** (Privilèges d'assistance invité) : la transaction sera autorisée à se poursuivre et correspondra aux politiques ultérieures pour les utilisateurs invités de tous les profils d'identification. • **Block Transactions** (Bloquer les transactions) : l'accès à Internet n'est pas permis aux utilisateurs qui ne peuvent pas être identifiés par ISE. • **Support Guest privileges** (Privilèges d'assistance invité) : cochez cette case pour accorder l'accès invité aux utilisateurs qui échouent à l'authentification en raison d'informations d'authentification non valides.

Domaine d'authentification	

Select a Realm or Sequence (Sélectionner un domaine ou une séquence) : choisissez un domaine ou une séquence d'authentification défini.

Select a Scheme (Sélectionner un schéma) : choisissez un schéma d'authentification :

- **Kerberos** : le client est authentifié de manière transparente au moyen de tickets Kerberos.
- **Basic** (De base) : le client demande toujours aux utilisateurs des informations d'authentification. Une fois que l'utilisateur a saisi les informations d'authentification, les navigateurs proposent généralement une case à cocher pour se souvenir des informations d'authentification fournies. Chaque fois que l'utilisateur ouvre le navigateur, le client demande des informations d'authentification ou renvoie les informations d'authentification précédemment enregistrées.

  Les informations d'authentification sont envoyées non sécurisées en texte clair (Base64). Une capture de paquets entre le client et Secure Web Appliance peut révéler le nom d'utilisateur et la phrase secrète.
- **NTLMSSP** : le client s'authentifie de manière transparente à l'aide de ses coordonnées de connexion Windows. L'utilisateur n'est pas invité à saisir ses informations d'authentification.

  Cependant, le client l'invite à saisir ses informations d'authentification dans les circonstances suivantes :

  - Échec des informations d'authentification Windows.
  - Le client ne fait pas confiance au Secure Web Appliance en raison des paramètres de sécurité du navigateur.

  Les informations d'authentification sont envoyées de manière sécurisée à l'aide d'une liaison tridirectionnelle (authentification de style condensé). La phrase secrète n'est jamais envoyée sur la connexion.
- **Header Based Authentication** (Authentification par en-tête) : le client et Secure Web Appliance considèrent l'utilisateur comme authentifié et ne lui demandent plus son authentification ou ses identifiants. La fonctionnalité X-Authenticated est opérante lorsque Secure Web Appliance agit en tant que périphérique en amont.

  Une fois l'authentification réussie, le périphérique en aval envoie le nom d'utilisateur et les groupes d'utilisateurs (facultatif) à Secure Web Appliance par le biais des en-têtes HTTP étendus X-Authenticated-User et X-Authenticated-Groups (facultatif).

  L'en-tête X-Authenticated-Groups sera pris en compte uniquement si vous configurez l'option **Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies** (Utiliser des groupes dans l'en-tête X-Authenticate-Groups/l'en-tête personnel pour les politiques correspondantes) sur l'appliance [**Network** > **Authentication** > **Edit Global Settings** (Réseau > Authentification > Modifier les paramètres globaux)].

  Remarque Les en-têtes X-Authenticated ne s'appliquent qu'aux politiques d'accès ou de routage. Cependant, l'association à une politique de déchiffrement du profil d'identification pour lequel l'option **Header**

	Based Authentication (Authentification basée sur l'en-tête) est activée ne produira pas de correspondance. • **Support Guest privileges** (Privilèges d'assistance invité) : cochez cette case pour accorder l'accès invité aux utilisateurs qui échouent à l'authentification en raison d'informations d'authentification non valides.
Domaine pour l'authentification de groupe	• **Select a Realm or Sequence** (Sélectionner un domaine ou une séquence) : choisissez un domaine ou une séquence d'authentification défini.

Authentication Surrogates (Substitutions d'authentification)	Indiquez comment les transactions seront associées à un utilisateur une fois l'authentification réussie (les options varient en fonction du mode de déploiement du proxy Web) : • **IP Address (Adresse IP)** : le proxy Web suit un utilisateur authentifié à une adresse IP particulière. Pour une identification transparente de l'utilisateur, sélectionnez cette option. • **Persistent Cookie** (Témoin persistant) : le proxy Web suit un utilisateur authentifié sur une application particulière en générant un témoin persistant pour chaque utilisateur et par application. La fermeture de l'application ne supprime pas le témoin. • **Session Cookie** (Témoin de session) : le proxy Web suit un utilisateur authentifié sur une application particulière en générant un témoin de session pour chaque utilisateur, par domaine et par application. (Cependant, lorsqu'un utilisateur fournit différents identifiants pour le même domaine à partir de la même application, le témoin est remplacé.) La fermeture de l'application supprime le témoin. • **No Surrogate** (Pas de substitution) : le proxy Web n'utilise pas de substitution pour mettre en cache les informations d'authentification et il suit un utilisateur authentifié pour chaque nouvelle connexion TCP. Lorsque vous choisissez cette option, l'interface Web désactive les autres paramètres qui ne s'appliquent plus. Cette option est disponible uniquement en mode de transfert explicite et lorsque vous désactivez le chiffrement des informations d'authentification dans la page Network > Authentication. • **Apply same surrogate settings to explicit forward requests** (Appliquer les mêmes paramètres de substitution aux demandes de transfert explicites) : cochez cette case pour appliquer la substitution utilisée pour les demandes transparentes aux demandes explicites; active automatiquement le chiffrement des identifiants. Cette option ne s'affiche que lorsque le proxy Web est déployé en mode transparent. **Remarque** • Vous pouvez définir une limite de délai d'expiration pour le remplaçant d'authentification pour toutes les demandes dans les paramètres d'authentification globaux. • Si vous avez configuré les profils d'identification de manière à utiliser différentes substitutions d'authentification (adresse IP, témoin persistant, témoin de session, etc.), l'accès est authentifié à l'aide de la substitution d'adresse IP même si l'accès correspond aux profils d'identification avec d'autres substitutions.

Étape 8 Dans la section de **Membership Definition** (Définition de l'appartenance), indiquez les paramètres d'appartenance appropriés selon la méthode d'identification choisie. Notez que toutes les options décrites dans ce tableau ne sont pas disponibles pour toutes les méthodes d'identification de l'utilisateur.

Membership Definition (Définition de l'appartenance)

Define Members by User Location (Définir les membres par emplacement d'utilisateur)	Configurez ce profil d'identification de sorte qu'il s'applique aux utilisateurs suivants : **utilisateurs locaux uniquement**, **utilisateurs à distance uniquement** ou les **deux**. Cette sélection affecte les paramètres d'authentification disponibles pour ce profil d'identification.
Define Members by Subnet (Définir les membres par sous-réseau)	Saisissez les adresses auxquelles ce profil d'identification doit s'appliquer. Vous pouvez utiliser des adresses IP, des blocs d'CIDR et des sous-réseaux. **Remarque** Si aucune information n'est saisie, le profil d'identification s'applique à toutes les adresses IP.
Define Members by Protocol (Définir les membres par protocole)	Sélectionnez les protocoles auxquels ce profil d'identification doit s'appliquer; sélectionnez toutes les réponses qui s'appliquent : • **HTTP/HTTPS** : s'applique à toutes les demandes qui utilisent HTTP ou HTTPS comme protocole sous-jacent, y compris FTP sur HTTP et tout autre protocole tunnelisé à l'aide de HTTP CONNECT. • **FTP natif** : s'applique aux demandes FTP natives uniquement. • **SOCKS** : s'applique uniquement aux politiques SOCKS
Define Members by Machine ID (Définir les membres par ID d'ordinateur)	• **Do Not Use Machine ID in This Policy** (Ne pas utiliser l'ID d'ordinateur dans cette politique) : l'utilisateur n'est pas identifié par l'ID d'ordinateur. • **Define User Authentication Policy Based on Machine ID** (Définir la politique d'authentification des utilisateurs en fonction de l'ID de l'ordinateur) : l'utilisateur est identifié principalement par l'ID de l'ordinateur. Cliquez sur la zone Machine Groups (Groupes d'ordinateurs) pour afficher la page des groupes d'ordinateurs autorisés. Pour chaque groupe que vous souhaitez ajouter, dans le champ Directory Search (Recherche dans le répertoire), commencez à taper le nom du groupe à ajouter, puis cliquez sur Add (Ajouter). Vous pouvez sélectionner un groupe, et cliquer sur Delete (Supprimer) pour le retirer de la liste. Cliquez sur Done (Terminé) pour revenir à la page précédente. Cliquez dans la zone Machine IDs (ID d'ordinateur) pour afficher la page des ordinateurs autorisés. Dans le champ Authorized Machines (Ordinateurs autorisés), saisissez les ID des ordinateurs à associer à la politique, puis cliquez sur Done (Terminé). **Remarque** L'authentification à l'aide de l'ID d'ordinateur est prise en charge uniquement en mode Connector et nécessite Active Directory.

Advanced (Niveau avancé)	Développez cette section pour définir les exigences d'appartenance supplémentaires. • **Proxy Ports** (Ports proxy) : indiquez un ou plusieurs ports proxy utilisés pour accéder au proxy Web. Entrez les numéros de port séparés par des virgules. Pour les connexions de transfert explicite, le port proxy est configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination. La définition des identités par port fonctionne mieux lorsque l'appliance est déployée en mode de transfert explicite ou lorsque les clients transfèrent explicitement les demandes à l'appliance. La définition des identités par port lorsque les demandes des clients sont redirigées de manière transparente vers l'appliance peut entraîner le refus de certaines demandes. • **URL Categories** (Catégories d'URL) : sélectionnez des catégories d'URL prédéfinies ou définies par l'utilisateur. L'appartenance pour les deux est exclue par défaut, ce qui signifie que le proxy Web ignore toutes les catégories, sauf si elles sont sélectionnées dans la colonne Add (ajouter). Si vous devez définir l'appartenance par catégorie d'URL, définissez-la uniquement dans le groupe Identity lorsque vous devez exclure des demandes d'authentification à cette catégorie. • **User Agents** (Agents utilisateurs) : définit l'appartenance au groupe de politiques des agents utilisateurs trouvés dans la demande du client. Vous pouvez sélectionner des agents généralement définis ou définir les vôtres à l'aide d'expressions régulières. Précisez également si ces spécifications d'agent utilisateur sont inclusives ou exclusives. Autrement dit, si la définition de l'appartenance inclut uniquement les agents utilisateur sélectionnés ou exclut expressément les agents utilisateurs sélectionnés

Étape 9 Envoyez et validez les modifications.

Prochaine étape

- Survol de l'acquisition des informations d'authentification de l'utilisateur final, à la page 101
- Présentation des tâches de gestion des demandes Web au moyen de politiques, à la page 249

Activer/désactiver une identité

Before you begin

- Sachez que la désactivation d'un profil d'identification entraîne la suppression de ce dernier des politiques associées.
- Sachez que la réactivation d'un profil d'identification ne le réassocie à aucune politique.

Étape 1 Choisissez **Web Security Manager** > **Identification Profiles** (Web Security Manager > Profils d'identification).

Étape 2 Cliquez sur un profil dans le tableau des profils d'identification pour ouvrir la page Identification Profile (Profil d'identification) pour ce profil.

Étape 3 Cochez ou décochez la case **Enable Identification Profile** (Activer le profil d'identification) immédiatement sous Client/User Identification Profile Settings (Paramètres du profil d'identification utilisateur/client).

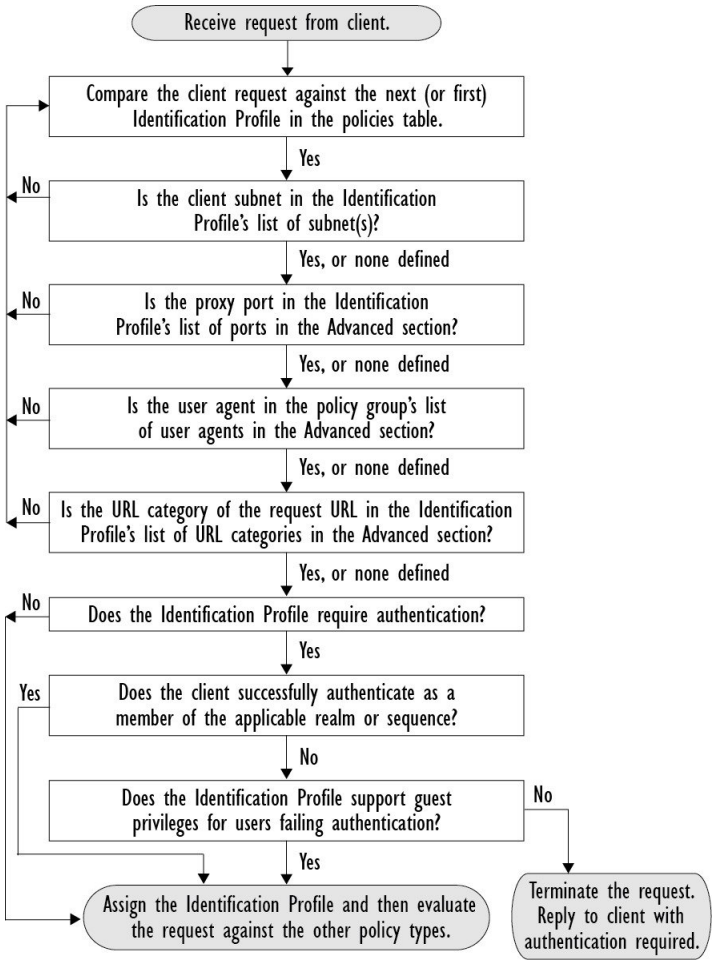
Étape 4 Envoyez et validez les modifications.

Profils d'identification et authentification

Le diagramme suivant montre comment le proxy Web évalue une demande d'un client par rapport à un profil d'identification lorsque ce dernier est configuré pour utiliser :

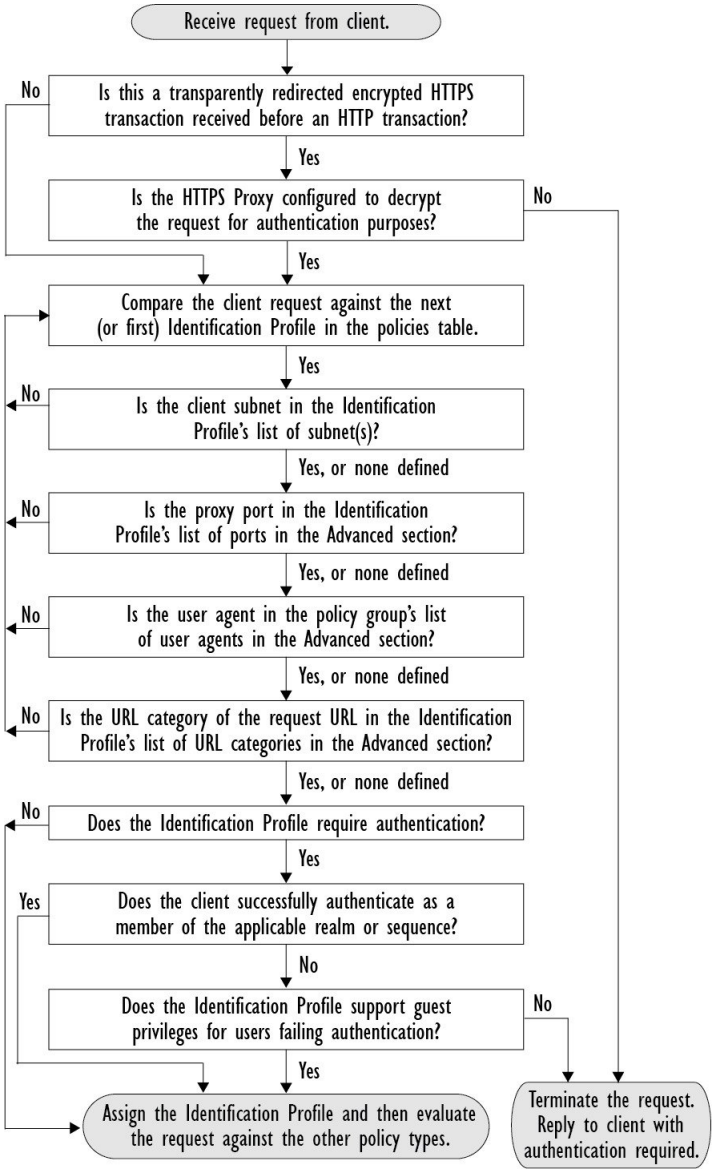
- Aucune substitution d'authentification
- Adresses IP comme substitutions d'authentification
- Témoins comme témoins d'authentification avec des demandes transparentes
- Les témoins comme substitutions d'authentification avec des demandes explicites et le chiffrement des identifiants sont activés

Figure 1: Profils d'identification et traitement d'authentification – Aucune substitution et substitutions basées sur IP



Le diagramme suivant montre comment le proxy Web évalue une demande d'un client par rapport à un profil d'identification lorsque le profil d'identification est configuré pour utiliser des témoins comme substitutions d'authentification, le chiffrement des informations d'identification est activé et la demande est explicitement transférée.

Figure 2: Profils d'identification et traitement d'authentification – Substitutions basées sur des témoins



Résolution de problèmes relatifs aux profils d'identification

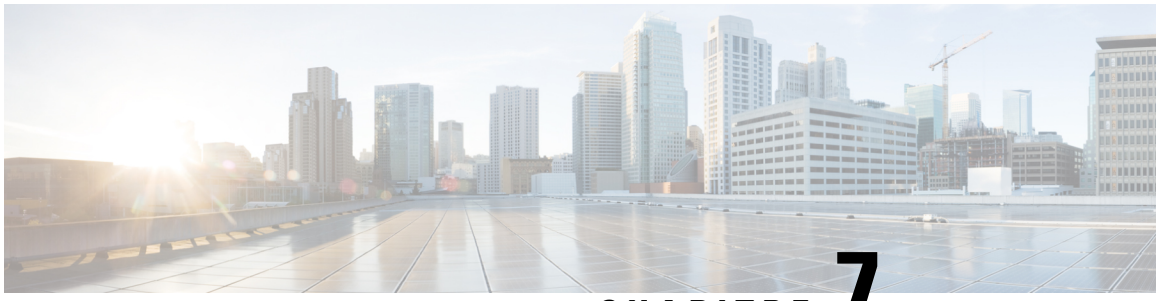
- Problèmes d'authentification de base, on page 636
- Problèmes de politique, on page 651
- La politique n'est jamais appliquée, on page 652
- Outil de résolution de problèmes liés aux politiques : Suivi des politiques, on page 653

• Problèmes de proxy en amont, on page 659

Résolution des problèmes relatifs aux types de substitution dans les profils d'identification

Lorsque l'appliance Cisco pour la sécurité du Web est configurée pour utiliser à la fois l'adresse IP et les substitutions d'authentification par témoin et que l'accès de l'utilisateur final correspond aux deux identités, l'adresse IP prévaut sur les substitutions d'authentification par témoin.

Dans un réseau comprenant des ordinateurs partagés et des ordinateurs individuels, il est recommandé de créer deux profils d'identification différents en fonction des adresses IP et des sous-réseaux, qui détermineront si des valeurs de substitution pour l'authentification par IP ou à l'aide de témoins sont utilisées.



CHAPITRE 7

Contrôle d'accès au logiciel-service (SaaS)

Cette rubrique contient les sections suivantes :

Survol du contrôle d’accès au logiciel-service (SaaS)

Secure Web Appliance utilise SAML (Security Assertion Markup Language) pour autoriser l’accès aux applications de logiciels-services. Il fonctionne avec des applications de logiciels-services qui sont strictement conformes à SAML version 2.0.

Le contrôle d’accès de logiciel-service Cisco vous permet de :

- Contrôlez quels utilisateurs peuvent accéder aux applications de logiciels-services et à partir d’où.
- Désactivez rapidement l’accès à toutes les applications d’applications-services lorsque les utilisateurs ne sont plus employés par l’entreprise.
- Réduisez le risque d’attaques d’hameçonnage qui demandent aux utilisateurs de saisir leurs informations d’identification d’utilisateur SaaS.
- Choisissez si les utilisateurs sont connectés de manière transparente (fonctionnalité de connexion unique) ou invités à saisir leur nom d’utilisateur et leur phrase secrète pour l’authentification.

Le contrôle d’accès SaaS fonctionne uniquement avec les applications SaaS qui nécessitent un mécanisme d’authentification pris en charge par Secure Web Appliance. À l’heure actuelle, le proxy Web utilise le mécanisme d’authentification « PasswordProtected Transport ».

Pour activer le contrôle d’accès au logiciel-service, vous devez configurer les paramètres sur Secure Web Appliance et l’application de logiciel-service :

Procedure

	Command or Action	Purpose
Étape 1	Configurez Secure Web Appliance comme fournisseur d'identité.	Configuration de l'appliance en tant que fournisseur d'identité, on page 166
Étape 2	Créez une politique d'authentification pour l'application de logiciel-service.	Création de politiques d'authentification d'applications de logiciel-service (SaaS), on page 168
Étape 3	Configurez l'application de logiciel-service pour la connexion unique.	Configuration de l'accès de l'utilisateur final à l'URL de connexion unique, on page 171
Étape 4	(Facultatif) Configurez plusieurs Secure Web Appliance.	Utilisation du contrôle d'accès au logiciel-service (SaaS) et de plusieurs appliances, on page 168

Configuration de l'appliance en tant que fournisseur d'identité

Lorsque vous configurez Secure Web Appliance comme fournisseur d'identité, les paramètres que vous définissez s'appliquent à toutes les applications de logiciels-services avec lesquelles il communique. Secure Web Appliance utilise un certificat et une clé pour signer chaque affirmation SAML qu'il crée.

Before you begin

- (Facultatif) Localisez un certificat (format PEM) et une clé pour la signature des Assertions SAML.
- Chargez le certificat dans chaque application de logiciel-service.

Étape 1 Choisissez **Network > Identity Provider for SaaS** ((Réseau > Fournisseur d'identité pour logiciel-service).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez la case **Enable SaaS Single Sign-on Service** (Activer le service de connexion unique SaaS).

Étape 4 Entrez un nom de domaine virtuel dans le champ **Identity Provider Domain Name** (Nom de domaine du fournisseur d'identité).

Étape 5 Saisissez un identifiant textuel unique dans le champ **Identity Provider Entity ID** (ID d'entité du fournisseur d'identité) (une chaîne au format URI est recommandée).

Étape 6 Chargez ou générez un certificat et une clé :

Méthode	Étapes supplémentaires
Charger un certificat et une clé	**a.** Sélectionnez **Use Uploaded Certificate and Key** (Utiliser le certificat et la clé téléchargés). **b.** Dans le champ **Certificate** (Certificat), cliquez sur Browse (Parcourir); localisez le fichier à télécharger. **Note** Le proxy Web utilise le premier certificat ou la première clé du fichier. Le fichier de certificat doit être au format PEM. Format DER non pris en charge. **c.** Dans le champ **Key** (Clé), cliquez sur Browse (Parcourir); localisez le fichier à télécharger. Si la clé est chiffrée, sélectionnez **Key is Encrypted** (La clé est chiffrée). **Note** La longueur de la clé doit être de 512, 1024 ou 2048 bits. Le fichier de clé privée doit être au format PEM. Format DER non pris en charge. **d.** Cliquez sur **Upload Files** (Charger des fichiers). **e.** Cliquez sur **Download Certificate** (Télécharger le certificat) pour télécharger une copie du certificat et la transférer vers les applications de logiciel-service avec lesquelles Secure Web Appliance communique.
Générer un certificat et une clé	**a.** Sélectionnez **Use Generate Certificate and Key** (Utiliser le certificat et la clé générés). **b.** Cliquez sur **Generate New Certificate and Key** (Générer un nouveau certificat et une nouvelle clé). **1.** Dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé), saisissez les informations à afficher dans le certificat de signature. **Note** Vous pouvez saisir n'importe quel caractère ASCII, à l'exception de la barre oblique (/) dans le champ Common Name (Nom commun). **2.** Cliquez sur **Generate** (Générer). **c.** Cliquez sur **Download Certificate** (Télécharger le certificat) pour transférer le certificat vers les applications de logiciel-service avec lesquelles Secure Web Appliance communiquera. **d.** (Facultatif) Pour utiliser un certificat signé, cliquez sur le lien **Download Certificate Signing Request** (DCSR) (Télécharger la demande de signature de certificat) pour envoyer une demande à une autorité de certification (CA). Après avoir reçu un certificat signé de l'autorité de certification, cliquez sur **Browse** (Parcourir) et accédez à l'emplacement du certificat signé. Cliquez sur **Upload Files** (Charger des fichiers). (bogue 37984)

Note Si l'appliance a à la fois un certificat et une paire de clés téléchargés et un certificat et une paire de clés générés, elle utilise uniquement le certificat et la paire de clés actuellement sélectionnés dans la section du certificat de signature.

Étape 7 Prenez note des paramètres lorsque vous configurez l'appliance en tant que fournisseur d'identité. Certains de ces paramètres doivent être utilisés lors de la configuration de l'application de logiciel-service pour la connexion unique.

Étape 8 Envoyez et validez les modifications.

What to do next

Après avoir spécifié le certificat et la clé à utiliser pour la signature des déclarations SAML, chargez le certificat dans chaque application de logiciel-service.

Thèmes connexes

- Configuration de l'accès de l'utilisateur final à l'URL de connexion unique, on page 171

Utilisation du contrôle d'accès au logiciel-service (SaaS) et de plusieurs appliances

Before you begin

Configuration de l'appliance en tant que fournisseur d'identité, on page 166

Étape 1 Configurez le même nom de domaine de fournisseur d'identité pour chaque Secure Web Appliance.

Étape 2 Configurez le même ID d'entité de fournisseur d'identité pour chaque Secure Web Appliance.

Étape 3 Chargez le même certificat et la même clé privée sur chaque appliance dans la page **Network > Identity Provider for SaaS** (Réseau > Fournisseur d'identité pour SaaS).

Étape 4 Chargez ce certificat dans chaque application de logiciel-service que vous configurez.

Création de politiques d'authentification d'applications de logiciel-service (SaaS)

Before you begin

- Créez les identités associées.
- Configurez le fournisseur d'identité, voir Configuration de l'appliance en tant que fournisseur d'identité, on page 166.
- Fournissez un certificat de signature de fournisseur d'identité et une clé : Network > Identity Provider for SaaS > Enable and Edit Settings (Réseau > Fournisseur d'identité pour logiciel-service > Activer et modifier les paramètres).
- Créez un domaine d'authentification, Domaines d'authentification, on page 115.

Étape 1 Choisissez **Web Security Manager > SaaS Policies** (Web Security Manager > Politiques SaaS)

Étape 2 Cliquez sur **Add Application** (Ajouter une application).

Étape 3 Configurez les paramètres.

Propriété	Description
Nom de l'application	Saisissez un nom pour identifier l'application de logiciel-service pour cette politique; chaque nom d'application doit être unique. Secure Web Appliance utilise le nom de l'application pour générer une URL de connexion unique.
Description	(Facultatif) Saisissez la description de cette politique SaaS.
Métadonnées pour le fournisseur de services	Configurez les métadonnées qui décrivent le fournisseur de services référencé dans cette politique. Vous pouvez soit décrire les propriétés du fournisseur de services manuellement, soit charger un fichier de métadonnées fourni par l'application de logiciel-service. Secure Web Appliance utilise les métadonnées pour déterminer comment communiquer avec l'application de logiciel-service (fournisseur de services) à l'aide de SAML. Contactez l'application de logiciel-service pour connaître les paramètres corrects de configuration des métadonnées. **Configure Keys Manually** (Configurer les clés manuellement) : si vous sélectionnez cette option, fournissez les éléments suivants : • **ID d'entité du fournisseur de services**. Saisissez le texte (généralement au format URI) que l'application de logiciel-service utilise pour s'identifier en tant que fournisseur de services. • **Name ID Format** (Format de l'ID du nom). Choisissez dans la liste déroulante le format que l'appliance doit utiliser pour identifier les utilisateurs dans l'assertion SAML envoyée aux fournisseurs de services. La valeur que vous entrez ici doit correspondre au paramètre correspondant configuré sur l'application de logiciel-service. • **Assertion Consumer Service URL** (URL de l'ACS (Assertion Consumer Service)). Entrez l'URL à laquelle Secure Web Appliance doit envoyer l'assertion SAML qu'elle crée. Lisez la documentation de l'application de logiciel-service pour déterminer la bonne URL à utiliser (également appelée URL de connexion). **Import File from Hard Disk** (Importer un fichier du disque dur) : si vous sélectionnez cette option, cliquez sur Parcourir, localisez le fichier, puis cliquez sur **Import** (Importer). **Note** Ce fichier de métadonnées est un document XML, selon la norme SAML, qui décrit une instance de fournisseur de services. Toutes les applications de logiciel-service n'utilisent pas de fichiers de métadonnées, mais pour celles qui le font, contactez le fournisseur d'applications de logiciel-service pour le fichier.

Propriété	Description
User Identification / Authentication for SaaS SSO (Identification/authentification de l'utilisateur pour SSO SaaS)	Préciser comment les utilisateurs sont identifiés ou authentifiés pour la connexion unique de logiciel-service : • Invitez toujours les utilisateurs à fournir leurs informations d'authentification locales. • Invitez les utilisateurs à fournir leurs identifiants d'authentification locale si le proxy Web a obtenu leurs noms d'utilisateur de manière transparente. • Enregistrez automatiquement les utilisateurs de logiciels-services à l'aide de leurs informations d'authentification locales. Choisissez le domaine ou la séquence d'authentification que le proxy Web doit utiliser pour authentifier les utilisateurs accédant à cette application de logiciel-service. Les utilisateurs doivent être membres du domaine d'authentification ou de la séquence d'authentification pour accéder avec succès à l'application de logiciel-service. Si un moteur de services d'identité est utilisé pour l'authentification et que LDAP a été sélectionné, le domaine sera utilisé pour les noms d'utilisateur SAML et le mappage d'attributs.
SAML User Name Mapping (Mappage des noms d'utilisateur SAML)	Précisez comment le proxy Web doit présenter les noms d'utilisateur pour le fournisseur de services dans l'assertion SAML. Vous pouvez transmettre les noms d'utilisateur tels qu'ils sont utilisés à l'intérieur de votre réseau (**pas de mappage**) ou vous pouvez modifier les noms d'utilisateurs internes dans un format différent à l'aide de l'une des méthodes suivantes : • **Requête LDAP**. Les noms d'utilisateur envoyés au fournisseur de services sont basés sur un ou plusieurs attributs de requête LDAP. Saisissez une expression contenant des champs d'attribut LDAP et du texte personnalisé facultatif. Vous devez mettre les noms d'attributs entre crochets. Vous pouvez inclure n'importe quel nombre d'attributs. Par exemple, pour les attributs LDAP « utilisateur » et « domaine », vous pourriez entrer <user>@<domain>.com. • **Mappage fixe des règles**. Les noms d'utilisateur envoyés au fournisseur de services sont basés sur le nom d'utilisateur interne et une chaîne fixe est ajoutée avant ou après le nom d'utilisateur interne. Entrez la chaîne fixe dans le champ **Expression Name** (Nom de l'expression), avec %s avant ou après la chaîne pour indiquer sa position dans le nom d'utilisateur interne.
SAML Attribute Mapping (Mappage des attributs SAML)	(Facultatif) Vous pouvez fournir à l'application de logiciel-service des informations supplémentaires sur les utilisateurs internes à partir du serveur d'authentification LDAP si l'application de logiciel-service l'exige. Mappez chaque attribut de serveur LDAP sur un attribut SAML.
Authentication Context (Contexte d'authentification)	Choisissez le mécanisme d'authentification que le proxy Web utilise pour authentifier ses utilisateurs internes. **Note** Le contexte d'authentification informe le fournisseur de services du mécanisme d'authentification utilisé par le fournisseur d'identité pour authentifier les utilisateurs internes. Certains fournisseurs de services exigent un mécanisme d'authentification particulier pour permettre aux utilisateurs d'accéder à l'application de logiciel-service. Si un fournisseur de services exige un contexte d'authentification qui n'est pas pris en charge par un fournisseur d'identité, les utilisateurs ne peuvent pas accéder au fournisseur de services en utilisant la connexion unique du fournisseur d'identité.

Étape 4 Envoyez et validez les modifications.

What to do next

Définissez les paramètres de connexion unique du côté de l'application de logiciel-service en utilisant les mêmes paramètres pour configurer l'application.

Configuration de l'accès de l'utilisateur final à l'URL de connexion unique

Après avoir configuré Secure Web Appliance comme fournisseur d'identité et créé une politique d'authentification d'application de logiciel-service pour l'application de logiciel-service (SaaS), l'appliance crée une URL de connexion unique (URL SSO). Secure Web Appliance utilise le nom de l'application configuré dans la politique d'authentification de l'application de logiciel-service pour générer l'URL de connexion unique; le format de l'URL de connexion unique est :

http://*IdentityProviderDomainName* /SSOURL/*ApplicationName*

Étape 1 Obtenez l'URL de connexion unique sur la page **Web Security Manager > SaaS Policies** (Web Security Manager > Politiques SaaS).

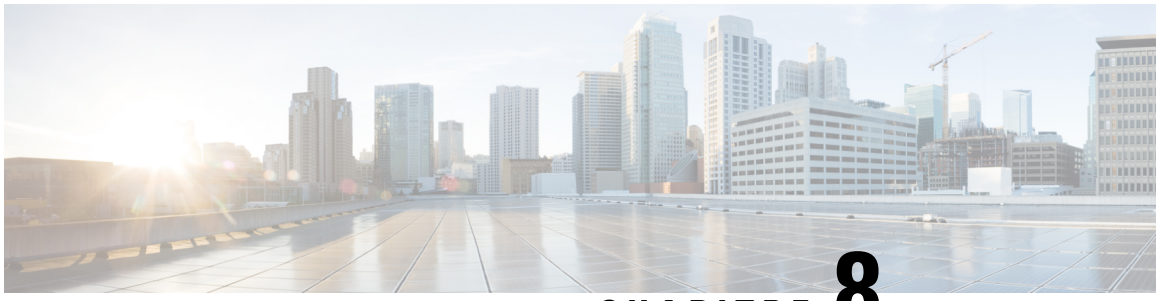
Étape 2 Rendre l'URL disponible pour les utilisateurs finaux en fonction du type de flux.

Étape 3 Si vous choisissez Identity provider initiated flow (Flux lancé par le fournisseur d'identité), l'appliance redirige les utilisateurs vers l'application de logiciel-service.

Étape 4 Si vous choisissez les flux initiés par le fournisseur de services, vous devez configurer cette URL dans l'application de logiciel-service.

- Toujours demander aux utilisateurs de logiciels-services de s'authentifier par proxy. Après avoir saisi des informations d'authentification valides, les utilisateurs sont connectés à l'application de logiciel-service.
- Enregistrez de manière transparente les utilisateurs de logiciels-services (SaaS). Les utilisateurs sont automatiquement connectés à l'application de logiciel-service.

  Note Pour obtenir un comportement de connexion unique utilisant des demandes de transfert explicites pour tous les utilisateurs authentifiés lorsque l'appliance est déployée en mode transparent, sélectionnez « **Apply same surrogate settings to explicit forward requests** » (Appliquer les mêmes paramètres de substitution pour les demandes de transfert explicites) lorsque vous configurez le groupe d'identités.



CHAPITRE 8

Intégrer le moteur de services de vérification des identités de Cisco (ISE)/contrôleur d'identité passif ISE (ISE-PIC)

Cette rubrique contient les sections suivantes :

Survol du moteur du service de vérification des identités Identity Services Engine (ISE) et du service du connecteur d'identité passive ISE (ISE-PIC)

Le moteur de services de vérification des identités (ISE) et le connecteur d'identité passive (ISE-PIC) de Cisco sont des applications qui s'exécutent sur des serveurs distincts de votre réseau pour fournir une gestion de l'identité améliorée. Secure Web Appliance peut accéder aux informations d'identité de l'utilisateur à partir d'un serveur ISE ou ISE-PIC. Lorsqu'ISE ou ISE-PIC est configuré, les informations sont récupérées (noms d'utilisateur et étiquettes Groupe sécurisé associée d'ISE, noms d'utilisateur et groupes Active Directory d'ISE-PIC) pour les profils d'identification configurés correctement, afin de permettre une identification transparente de l'utilisateur dans les politiques configurées d'utiliser ces profils.

- Vous pouvez élaborer des politiques d'accès à l'aide d'étiquettes Groupe sécurisé et de groupes Active Directory.
- Pour les utilisateurs qui échouent à l'identification transparente avec ISE/ISE-PIC, vous pouvez configurer l'authentification de secours avec des domaines basés sur Active Directory. Consultez Authentification secondaire, on page 177.

- Vous pouvez configurer l'authentification des utilisateurs dans les environnements de bureaux virtuels (Citrix, services de bureau partagé ou à distance de Microsoft, etc.). Consultez Authentification des utilisateurs VDI (Virtual Desktop Infrastructure) dans les intégrations ISE/ISE-PIC, on page 188.

Note

- Le service ISE/ISE-PIC n'est pas disponible en mode Connector.
- ISE/ISE-PIC version 2.4 et PxGrid version 2.0 sont pris en charge.
- La page de configuration ISE de l'interface Web de Secure Web Appliance est utilisée pour configurer les serveurs ISE ou ISE-PIC, pour charger des certificats et pour la connexion aux services ISE ou ISE-PIC. Les étapes de configuration d'ISE ou d'ISE-PIC sont similaires, et tous les détails spécifiques aux configurations ISE-PIC ont été mentionnés, le cas échéant.

Pour en savoir plus sur le tableau de prise en charge des versions de Cisco Secure Web Appliance ISE, consulter les informations sur le tableau de compatibilité ISE.

Table 5: Secure Web Appliance - Tableau de prise en charge de la gamme ISE

Modèles	Échelle de session sans groupe AD activé	Échelle de session avec le groupe AD activé	
-	Nombre maximal de sessions actives prises en charge	Nombre maximal de sessions actives prises en charge	Nombre maximal de terminaux pris en charge (Entrées du groupe AD pour chaque utilisateur et point d'extrémité dans la base de données ISE.)
S680*, S690, S695	200 000	125 000	400 000
S380*, S390, S600V	150 000	50 000	150 000
S190, S195, S300V	50 000	50 000	75 000
S100V	50 000	40 000	50 000

Note *Les modèles S380 et S680 ne sont pas pris en charge.

Thèmes connexes

- À propos de pxGrid, on page 175
- À propos du déploiement et du basculement du serveur ISE/ISE-PIC, on page 175

À propos de pxGrid

La plateforme Platform Exchange Grid (pxGrid) de Cisco permet la collaboration entre les composants de l'infrastructure réseau, notamment les systèmes de supervision de la sécurité et de détection du réseau, les plateformes de gestion de l'identité et des accès, etc. Ces composants peuvent utiliser pxGrid pour échanger des informations par une méthode de publication/abonnement.

Il existe essentiellement trois composants pxGrid : le serveur de publication pxGrid, le client pxGrid et le contrôleur pxGrid.

- pxGrid Publisher : Fournit des informations sur le ou les clients pxGrid.
- Client pxGrid : tout système, comme le Secure Web Appliance, qui s'abonne aux informations publiées; dans ce cas, la balise de groupe de sécurité (SGT), les groupes Active Directory, le groupe d'utilisateurs et les informations de profilage.
- Contrôleur pxGrid : Dans ce cas, le nœud pxGrid ISE/ISE-PIC qui contrôle les processus d'enregistrement/de gestion et de sujet/abonnement du client.

Des certificats approuvés sont requis pour chaque composant et ceux-ci doivent être installés sur chaque plateforme hôte.

À propos du déploiement et du basculement du serveur ISE/ISE-PIC

La configuration d'un seul nœud ISE/ISE-PIC est appelée un déploiement autonome, et ce nœud unique exécute le service d'administration et des politiques. Pour prendre en charge le basculement et améliorer les performances, vous devez configurer plusieurs nœuds ISE/ISE-PIC dans un déploiement distribué. La configuration ISE/ISE-PIC distribuée minimale requise pour prendre en charge le basculement ISE/ISE-PIC sur votre Secure Web Appliance est de :

- Deux nœuds pxGrid
- Deux nœuds d'administration
- Un nœud de service de politique

Cette configuration est appelée « déploiement dans un réseau de taille moyenne » dans le *Guide d'installation du matériel de Cisco Identity Services Engine*. Reportez-vous à la section sur les déploiements réseau de ce guide d'installation pour en savoir plus.

Thèmes connexes

- Certificats ISE/ISE-PIC, on page 176
- Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 177
- Se connecter aux services ISE/ISE-PIC, on page 180
- Résolution des problèmes du service Cisco de vérification des identités, on page 188

Certificats ISE/ISE-PIC

Note Cette section décrit les certificats nécessaires pour une connexion ISE/ISE-PIC. Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 177 fournit des informations détaillées sur ces certificats. Certificate Management, on page 608 fournit des informations générales sur la gestion des certificats pour AsyncOS.

Un ensemble de deux certificats est requis pour l'authentification mutuelle et la communication sécurisée entre le Secure Web Appliance et chaque serveur ISE/ISE-PIC :

- **Certificat client d'appliance Web** – Utilisé par le serveur ISE/ISE-PIC pour authentifier Secure Web Appliance.
- **Certificat ISE pxGrid** : utilisé par Secure Web Appliance pour authentifier un serveur ISE/ISE-PIC sur le port 5222 pour Secure Web Appliance - Abonnement aux données ISE/ISE-PIC (requêtes publication/abonnement continues sur le serveur ISE/ISE-PIC).

Ces deux certificats peuvent être signés par l'autorité de certification (CA) ou autosignés. AsyncOS offre la possibilité de générer un certificat client d'appareil Web autosigné ou une requête de signature de certificat (CSR), si un certificat signé par une autorité de certification est nécessaire. De même, le serveur ISE/ISE-PIC offre la possibilité de générer des certificats pxGrid ISE/ISE-PIC autosignés, ou des requêtes de signature de certificat (CSR), si des certificats signés par une autorité de certification sont nécessaires.

Thèmes connexes

- Utilisation de certificats autosignés, on page 176
- Utilisation de certificats signés par une autorité de certification, on page 177
- Survol du moteur du service de vérification des identités Identity Services Engine (ISE) et du service du connecteur d'identité passive ISE (ISE-PIC), on page 173
- Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 177
- Se connecter aux services ISE/ISE-PIC, on page 180

Utilisation de certificats autosignés

Lorsque des certificats autosignés sont utilisés sur le serveur ISE/ISE-PIC, le certificat ISE/ISE-PIC pxGrid développé sur le serveur ISE/ISE-PIC, ainsi que le certificat client d'appliance Web développé sur le Secure Web Appliance doivent être ajoutés dans le magasin des certificats approuvés sur le serveur ISE/ISE-PIC [sur **ISE** - Administration > Certificates > Trusted Certificates > Import (Administration > Certificats > Certificats approuvés > Importer); sur **ISE-PIC** - Certificates > Trusted Certificates > Import (Certificats > Certificats approuvés > Importer)].

Caution Nous vous déconseillons d'utiliser des certificats autosignés pour l'authentification, car leur sécurité n'est pas aussi élevée que les autres méthodes d'authentification. De plus, un certificat autosigné ne prend pas en charge la politique de révocation.

Utilisation de certificats signés par une autorité de certification

Dans le cas de certificats signés par une autorité de certification :

- Sur le serveur ISE/ISE-PIC, assurez-vous que le certificat racine de l'autorité de certification approprié pour le certificat client d'appliance Web est présent dans le magasin des certificats approuvés [Administration > Certificates > Trusted Certificates (Administration > Certificats > Certificats approuvés)].
- Sur le Secure Web Appliance, assurez-vous que les certificats racine de l'autorité de certification appropriés sont présents dans la liste des certificats approuvés [Network > Certificate Management > Manage Trusted Root Certificates (Réseau > Gestion des certificats > Gérer les certificats racine approuvés)].
- Sur la page de moteur ISE (Network (Réseau) > Identity Services Engine), veillez à télécharger le certificat racine de l'autorité de certification pour le certificat ISE/ISE-PIC pxGrid.

Authentification secondaire

Pour les informations utilisateur qui ne sont pas disponibles dans ISE/ISE-PIC, vous pouvez configurer une authentification de secours. Assurez-vous de disposer des éléments suivants pour réussir l'authentification de secours.

- Profil d'identification configuré avec une option de repli de domaine basé sur Active Directory.
- Politique d'accès avec le profil d'identification approprié qui contient l'option de secours.

Tâches relatives à l'intégration du service ISE/ISE-PIC

Note

- ISE/ISE-PIC version 2.4 et PxGrid version 2.0 sont pris en charge.
- Pour continuer à utiliser les politiques d'accès existantes avec ISE-PIC, vous devez modifier les profils d'identification respectifs pour utiliser ISE-PIC et identifier les utilisateurs de manière transparente. Cela s'applique aux profils d'identification qui utilisent CDA. Si vous migrez d'une identification CDA à une identification basée sur ISE-PIC, vous devez modifier les profils d'identification respectifs.

Note

- Reconfigurez ISE sur Secure Web Appliance si vous effectuez une mise à niveau depuis AsyncOS 11.5 ou versions antérieures vers AsyncOS 11.7 ou versions ultérieures.
- Le certificat doit être généré par le périphérique ISE/ISE-PIC et le certificat généré doit être téléchargé vers Secure Web Appliance.

Étape	Tâche	Liens vers les rubriques et les procédures
1	Générer un certificat à l'aide d'un périphérique ISE/ISE-PIC	Génération de certificats par ISE/ISE-PIC, on page 178
2	Configurez l'ISE/ISE-PIC pour l'accès Secure Web Appliance.	Configuration du serveur ISE/ISE-PIC pour l'accès Secure Web Appliance , on page 179
3	Configurez et activez les services ISE/ISE-PIC dans Secure Web Appliance.	Se connecter aux services ISE/ISE-PIC, on page 180
4	Si le certificat client Secure Web Appliance est autosigné, importez-le dans ISE/ISE-PIC.	Importer le certificat client Secure Web Appliance autosigné dans le déploiement autonome ISE/ISE-PIC, on page 182 Importer le certificat client Secure Web Appliance autosigné dans le déploiement distribué ISE/ISE-PIC, on page 182
5	Si nécessaire, configurez la journalisation dans Secure Web Appliance.	Configuration de la journalisation pour ISE/ISE-PIC, on page 184
6	Obtenez les détails du serveur ISE/ISE-PIC ERS.	Acquisition de détails sur le serveur ERS ISE/ISE-PIC provenant d'ISE/ISE-PIC, on page 184

Thèmes connexes

- Survol du moteur du service de vérification des identités Identity Services Engine (ISE) et du service du connecteur d'identité passive ISE (ISE-PIC), on page 173
- Certificats ISE/ISE-PIC, on page 176
- Résolution des problèmes du service Cisco de vérification des identités, on page 188

Génération de certificats par ISE/ISE-PIC

Remarque Le certificat généré par le périphérique ISE ou ISE-PIC doit être au format PKCS12.

- **ISE/ISE-PIC :**

Étape 1 Choisissez **Work Centres** > **PassiveID** > **Subscribers** > **Certificates** (Postes de travail > PassiveID > Abonnés > Certificats).

Étape 2 Choisissez le **format PKCS 12** dans la liste déroulante **Certificate Download Format** (Format de téléchargement de certificat). Saisissez d'autres informations appropriées dans l'onglet **Certificates** (Certificats), puis générez un certificat pxGrid.

Étape 3 Extrayez l'autorité de certification racine, le certificat client de l'appliance Web et la clé client de l'appliance Web du fichier XXX.pk12 généré à l'aide de la commande `openssl` :

- **Autorité de certification racine :** openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem
- **Certificat client pour appliance Web :** openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem
- **Clé client de l'appliance Web :** openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem

Remarque Utilisez le même mot de passe de certificat que celui que vous avez saisi sur l'interface Web d'ISE lors de l'exécution de l'étape 2.

Remarque Suivez les mêmes étapes pour générer l'autorité de certification racine secondaire, le certificat client de l'appliance Web et la clé client de l'appliance Web au moyen du serveur ISE secondaire/de basculement.

Configuration du serveur ISE/ISE-PIC pour l'accès Secure Web Appliance

- **ISE**
  - Chaque serveur ISE doit être configuré pour permettre aux abonnés au sujet de l'identité (comme Secure Web Appliance) d'obtenir le contexte de session en temps réel.
    1. Choisissez **Administration** > **pxGrid Services** > **Settings** > **pxGrid Settings** (Administration > Services pxGrid > Paramètres > Paramètres pxGrid).
    2. Assurez-vous que la case **Automatically approve new certificate-based accounts** (Approuver automatiquement les nouveaux comptes basés sur des certificats) est cochée.

    Supprimez tous les anciens Secure Web Appliance configurés qui ne participent à aucune authentification à l'aide d'ISE/ISE-PIC.

    Assurez-vous que le pied de page du serveur ISE est vert et indique **Connected to pxGrid** (Connecté à pxGrid).

- **ISE-PIC**
  - Chaque serveur ISE-PIC doit être configuré pour permettre aux abonnés à la rubrique d'identité (comme Secure Web Appliance) d'obtenir le contexte de session en temps réel.
    1. Choisissez **Subscribers** > **Settings** (Abonnés > Paramètres).
    2. Assurez-vous que la case **Automatically approve new certificate-based accounts** (Approuver automatiquement les nouveaux comptes basés sur des certificats) est cochée.

    Supprimez tous les anciens Secure Web Appliance configurés qui ne participent à aucune authentification à l'aide d'ISE/ISE-PIC.

    Assurez-vous que le pied de page du serveur ISE est vert et indique **Connected to pxGrid** (Connecté à pxGrid).

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Se connecter aux services ISE/ISE-PIC

Note Si l'administrateur ISE, les certificats pxGrid et MNT sont signés par votre certificat d'autorité de certification racine, téléchargez le certificat de l'autorité de certification racine dans les champs de certificat de nœud ISE pxGrid sur l'appliance [**Network** > **Identity Services Engine** (Réseau > Identity Services Engine)].

Before you begin

- Assurez-vous que chaque serveur ISE/ISE-PIC est configuré correctement pour l'accès Secure Web Appliance; voir Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 177.
- Obtenir des clés et des certificats valides liés à ISE/ISE-PIC. Voir les informations connexes dans Génération de certificats par ISE/ISE-PIC, on page 178.
- Importez le fichier RootCA.pem obtenu dans Secure Web Appliance [**Network** > **CertificateManagement** > **TrustedRootCertificate** > **Client on ManageTrustedRootCertificate** (Réseau > CertificateManagement > TrustedRootCertificate > Client sur ManageTrustedRootCertificate)]. Pour extraire l'autorité de certification racine, le certificat client de l'appliance Web et la clé du client de l'appliance Web du fichier XXX.pk12 généré, consultez Génération de certificats par ISE/ISE-PIC, on page 178.

Note Suivez la même procédure pour le fichier rootCA.pem extrait du fichier XXXX.pk12 secondaire (si le serveur ISE secondaire ou de basculement est disponible).

- La page de configuration ISE de l'interface Web de Secure Web Appliance est utilisée pour configurer les serveurs ISE ou ISE-PIC, pour charger des certificats et pour la connexion aux services ISE ou ISE-PIC. Les étapes de configuration d'ISE ou d'ISE-PIC sont identiques, et tous les détails spécifiques aux configurations ISE-PIC ont été mentionnés, le cas échéant.
- Activez ERS si vous concevez des politiques d'accès à l'aide des groupes Active Directory fournis par ISE/ISE-PIC.

Étape 1 Choisissez **Network > Identification Service Engine** (Réseau > Moteur du service d'identification).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Si vous configurez ISE/ISE-PIC pour la première fois, cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Étape 3 Cochez la case **Enable ISE service** (Activer le service ISE).

Étape 4 Identifiez le **nœud d'administration principal** à l'aide de son nom d'hôte ou de son adresse IPv4 et saisissez les informations suivantes dans l'onglet du **nœud pxGrid ISE principal** sur Secure Web Appliance.

a) Fournissez un **certificat de nœud pxGrid ISE** pour un Secure Web Applianceabonnement données -ISE/ISE-PIC (requêtes continues au serveur ISE/ISE-PIC).

Recherchez et sélectionnez le certificat (ou la chaîne de certificats qui comprend tout certificat intermédiaire) généré à partir du serveur ISE principal en tant qu'autorité de certification racine (c.-à-d. RootCA.pem); consultez

Génération de certificats par ISE/ISE-PIC, on page 178, puis cliquez sur **Upload File**(Charger le fichier). Voir Chargement d'un certificat et d'une clé, on page 610 pour de plus amples informations.

Étape 5 Si vous utilisez un deuxième serveur ISE/ISE-PIC pour le basculement, identifiez son **nœud d'administration principal** à l'aide de son nom d'hôte ou de son adresse IPv4 et fournissez les informations suivantes dans l'onglet **Secondary ISE pxGrid Node** (Nœud pxGrid ISE secondaire) sur le Secure Web Appliance en utilisant son nom d'hôte ou son adresse IPv4 .

a) Fournissez le **certificat de nœud ISE secondaire pxGrid**.

Recherchez et sélectionnez le certificat (ou la chaîne de certificats qui comprend tous les certificats intermédiaires) qui est généré à partir du serveur ISE secondaire en tant qu'autorité de certification racine (c.-à-d. **RootCA.pem**); consultez Génération de certificats par ISE/ISE-PIC, on page 178, puis cliquez sur **Upload File** (Charger le fichier); consultez Chargement d'un certificat et d'une clé, on page 610 pour obtenir des renseignements supplémentaires.

Note Pendant le basculement du serveur ISE principal vers les serveurs ISE secondaires, tout utilisateur qui ne figure pas dans le cache SGT ISE existant devra s'authentifier ou se verra attribuer une autorisation d'invité, selon votre configuration de Secure Web Appliance. Une fois le basculement ISE terminé, l'authentification ISE normale reprend.

Étape 6 Fournissez un **certificat client d'appliance Web** pour l'authentification mutuelle des serveurs Secure Web Appliance-ISE/ISE-PIC :

- **Utiliser le certificat et la clé chargés**

  Pour le certificat et la clé, cliquez sur Choose (Choisir) et accédez au fichier correspondant.

  Note Sélectionnez et chargez les fichiers publicCert.pem et privateKey.pem générés par le biais du périphérique ISE/ISE-PIC. Consultez Génération de certificats par ISE/ISE-PIC, on page 178.

  Si la **clé est chiffrée**, cochez cette case.

  Cliquez sur **Upload Files** (Charger des fichiers). (Voir Chargement d'un certificat et d'une clé, on page 610 pour en savoir plus sur cette option.)

Étape 7 Activez le service ISE SGT eXchange Protocol (SXP).

Pour plus d'informations sur l'activation de Secure Web Appliance en vue de récupérer les rubriques de liaison SXP à partir des services ISE, consultez Activation du protocole ISE-SXP pour le mappage des adresses SGT vers les adresses IP, on page 186.

Étape 8 Activez le service ERS (External Restful Service) ISE.

- Saisissez le nom d'utilisateur et le mot de passe de l'administrateur ERS. Voir Acquisition de détails sur le serveur ERS ISE/ISE-PIC provenant d'ISE/ISE-PIC, on page 184.
- Si le service ERS est disponible sur les mêmes nœuds ISE/ISE-PIC pxGrid, cochez la case **Server name same as ISE pxGrid Node** (Nom de serveur identique au nœud pxGrid ISE/ISE). Sinon, entrez les noms d'hôte ou les adresses IPv4 des serveurs principal et secondaires (si ceux-ci sont configurés).

Étape 9 Cliquez sur **Start Test** (Démarrer le test) pour tester la connexion avec le ou les nœuds pxGrid ISE/ISE-PIC.

Étape 10 Cliquez sur **Submit** (Soumettre).

What to do next

- Classification des utilisateurs et logiciels clients, on page 153
- Créer des politiques pour contrôler les demandes Internet, on page 247

Informations connexes

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html, en particulier « Comment intégrer Cisco Secure Web Appliance à l'aide d'ISE/ISE-PIC et TrustSec à l'aide de pxGrid. »

Importer le certificat client Secure Web Appliance autosigné dans le déploiement autonome ISE/ISE-PIC

Les étapes élémentaires sont les suivantes :

- **Nœud d'administration ISE**
  - Choisissez **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Administration > Certificats > Gestion des certificats > Certificats approuvés > Importer).

  Assurez-vous que les options suivantes sont cochées :
  - Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
  - Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
  - Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)
- **Nœud d'administration ISE-PIC**
  - Choisissez **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Certificats > Gestion des certificats > Certificats approuvés > Importer).

    Assurez-vous que les options suivantes sont cochées :
    - Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
    - Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
    - Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Importer le certificat client Secure Web Appliance autosigné dans le déploiement distribué ISE/ISE-PIC

Les étapes élémentaires sont les suivantes :

- **Nœud d'administration ISE :**
  - Choisissez **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Administration > Certificats > Gestion des certificats > Certificats approuvés > Importer).

Assurez-vous que les options suivantes sont cochées :

- Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
- Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
- Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)

- **Nœud d'administration ISE-PIC :**
  - Choisissez **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Certificats > Gestion des certificats > Certificats approuvés > Importer).

    Assurez-vous que les options suivantes sont cochées :
    - Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
    - Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
    - Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Remarque Dans un déploiement ISE distribué, Secure Web Appliance communique avec les nœuds MNT, PAN et PxGrid. Dans ce cas, les certificats ou l'émetteur de tous les certificats doivent être disponibles dans le « certificat racine extrait », c'est-à-dire dans l'autorité de certification racine qui est générée par le périphérique ISE ou ISE-PIC. Consultez Génération de certificats par ISE/ISE-PIC, à la page 178.

Étape 1 Suivez les étapes dans Génération de certificats par ISE/ISE-PIC, à la page 178 pour générer l'autorité de certification racine, le certificat client de l'appliance Web et la clé du client de l'appliance Web.

Étape 2 Sur le **nœud d'administration ISE/ISE-PIC**, exportez manuellement les certificats auto-signés en sélectionnant **ISE/ISE-PIC** > **Administration** > **System** > **Certificates** > **System Certificates** (ISE /ISE-PIC > Administration > Système > Certificats > Certificats système)

1. Sélectionnez un certificat qui est « Utilisé par » parmi les suivants : [pxGrid, EAP Authentication, Admin, Portal, RADIUS DTLS].
2. Cliquez sur **Export** (Exporter) et enregistrez le fichier .pem généré.

Répétez les étapes ci-dessus pour tous les nœuds distribués ISE/ISE-PIC.

Étape 3 Ajoutez manuellement les fichiers de certificat téléchargés dans RootCA.pem à l'aide des commandes `openssl`. Pour générer et extraire des fichiers de certificat dans rootCA.pem à l'aide du périphérique ISE/ISE-PIC, consultez Génération de certificats par ISE/ISE-PIC, à la page 178.

1. Exécutez la commande suivante sur le certificat téléchargé :

```
Example:

openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:

Exemple (sortie) :
```

```
Issuer: CN=isehcamnt2.node
Subject: CN=isehcamnt2.node
```

2. Modifiez le contenu comme suit :

```
Example:
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

3. Ajoutez la ligne suivante dans le fichier RacineCA.pem :

```
Attributs du panier : <Empty Attributes>
```

4. Ajoutez l'objet et l'émetteur de l'étape (2) dans le fichier RootCA.pem avec l'étape (3).

```
Example:
Bag Attributes: <Empty Attributes>
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

5. Copiez tout le contenu du fichier de certificat téléchargé et collez-le à la fin de l'autorité de certification racine, après les données de l'étape (4).

   Répétez les étapes (1) à (5) pour tous les certificats téléchargés de nœuds ISE/ISE-PIC distribués et enregistrez le certificat RacineCA modifié.

Étape 4 Chargez le fichier RootCA.pem modifié dans la page de configuration ISE de Secure Web Appliance. Consultez Se connecter aux services ISE/ISE-PIC, à la page 180.

Configuration de la journalisation pour ISE/ISE-PIC

- Ajoutez le champ personnalisé %m aux journaux d'accès pour consigner le mécanisme d'authentificationPersonnalisation des journaux d'accès, on page 523 : .
- Vérifiez que le journal de service ISE/ISE-PIC a été créé; si ce n'est pas le cas, créez-le —Ajout et modification d'abonnements aux journaux, on page 491.
- Définissez les profils d'identification qui accèdent à ISE/ISE-PIC pour l'identification et l'authentification des Classification des utilisateurs et logiciels clients.
- Configurez des politiques d'accès qui utilisent l'identification ISE/ISE-PIC pour définir les critères et les actions relatives aux demandes des utilisateursConfiguration des politiques.

Acquisition de détails sur le serveur ERS ISE/ISE-PIC provenant d'ISE/ISE-PIC

- Activez l'API REST de Cisco ISE dans ISE/ISE-PIC (les API utilisent le port HTTPS 9060).

Note Vous devez activer le service externe de repos (ERS) d'ISE sur Secure Web Appliance [Network > Identity Services Engine (Réseau > Moteur ISE)] pour configurer des politiques de sécurité basées sur les groupes. Cela s'applique à la version 11.7 et ultérieure.

- **ISE**

- Choisissez **Administration** > **Settings** > **ERS Settings** > **ERS settings for primary admin node** > **Enable ERS** (Administration > Paramètres > Paramètres ERS pour le nœud d'administration principal > Activer ERS).

  Activez **ERS for Read for All Other Nodes** (Lecture ERS pour tous les autres nœuds), s'il y a des nœuds secondaires.

- **ISE-PIC**
  - Choisissez **Settings** > **ERS Settings** > **Enable ERS** (Paramètres > Paramètres ERS) > Activer ERS).

- Assurez-vous d'avoir créé un administrateur ISE avec le bon groupe de services RESTful externes. Le groupe d'administration des services RESTful externe a un accès complet à toutes les API du serveur ERS (GET, POST, DELERE, PUT). Cet utilisateur peut créer, lire, mettre à jour et supprimer des demandes d'API ERS. L'opérateur de services RESTful externe dispose d'un accès en lecture seule (demande GET uniquement).
  - **ISE**
    - Choisissez **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users** (Administration > Système > Accès admin > Administrateurs > Utilisateurs admin).
  - **ISE-PIC**
    - Choisissez **Administration** > **Admin Access** > **Admin Users** (Administration > Accès admin > Utilisateurs admin).

Si le service ERS est disponible sur des serveurs distincts, et non sur les nœuds pxGrid ISE/ISE-PIC, vous aurez besoin des noms d'hôte ou adresses IPv4 des serveurs principal et secondaire (si configurés).

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Configurer l'intégration d'ISE-SXP

Cette section aborde les points suivants :

À propos du protocole ISE-SXP pour le mappage SGT vers les adresses IP

SGT Exchange Protocol (SXP) est un protocole développé pour propager les liaisons IP-SGT sur les périphériques réseau. Une balise de groupe de sécurité (SGT) spécifie les privilèges d'une source de trafic dans un réseau sécurisé.

Vous pouvez intégrer le déploiement de Cisco Identity Services Engine (ISE) à Cisco Secure Web Appliance pour une authentification passive. Secure Web Appliance peut s'abonner aux mappages SXP à partir d'ISE. ISE utilise SXP pour propager la base de données de mappage SGT-adresses IP vers les périphériques gérés. Lorsque vous configurez Secure Web Appliance pour utiliser le serveur ISE, vous activez l'option pour qu'il écoute le sujet SXP d'ISE. Ainsi, Secure Web Appliance en apprendra davantage sur les serveurs SGT et les mappages d'adresses IP directement à partir d'ISE.

Secure Web Appliance génère des adresses IP d'authentification d'utilisateur fictives, qui comprennent l'adresse IP de la grappe ISE ainsi que l'adresse IP du client. Par conséquent, plusieurs adresses IP de clients peuvent être authentifiées sur l'adresse IP de la grappe.

Lignes directrices et limites relatives à la licence

Le protocole ISE-SXP pour le mappage SGT-adresses IP comprend les directives et les limites suivantes :

- Les terminaux compatibles avec IPv6 ne sont pas pris en charge dans la version 14.5 de Secure Web Appliance.
- Dans Secure Web Appliance la version 14.5, les noms d'utilisateur et le mappage de groupe ne sont pas disponibles dans les mappages SGT-adresses IP. Par conséquent, l'administrateur ne peut pas créer de politiques basées sur les utilisateurs et les groupes ISE dans Secure Web Appliance. Cependant, il peut être créé avec des balises SGT.
- Pour planifier l'horodatage de redémarrage pour le processus de téléchargement en bloc, vous devez configurer l'heure au format HH::MM dans les 24 heures pour redémarrer le processus configuré.

Remarque Il est recommandé de configurer l'heure à laquelle le processus d'authentification de l'utilisateur est indiqué comme étant inférieur à la journée. Par exemple, à 00:00 heure.

Prérequis

Le protocole ISE-SXP pour le mappage SGT-à-adresse IP nécessite la condition préalable suivante :

- Nécessite un certificat racine approuvé. Pour ajouter un certificat racine approuvé, consultez Gestion des certificats racine approuvés.

Activation du protocole ISE-SXP pour le mappage des adresses SGT vers les adresses IP

Tous les mappages définis dans ISE, y compris les mappages SGT-adresses IP peuvent être publiés par SXP. Vous pouvez récupérer les informations d'ISE-SXP à l'aide des mécanismes suivants :

- Téléchargement en bloc : après le redémarrage d'un processus géré, Secure Web Appliance envoie la demande de téléchargement en bloc au nœud de l'agrégateur ISE afin d'obtenir des informations sur toutes les entrées ISE-SXP disponibles sur le nœud de l'agrégateur. Vous pouvez planifier l'horodatage du redémarrage à l'aide de l'interface de ligne de commande AsyncOS.

- Mise à jour incrémentielle Secure Web Appliance : s'abonne sur un connecteur Web pour recevoir des messages de mise à jour incrémentielle. Il existe deux types de messages :
  - Create (Créer) : pour toutes les entrées nouvellement créées
  - Delete (Supprimer) : pour toutes les entrées SXP mises à jour

Remarque Secure Web Appliance reçoit deux messages (Delete suivi de Create) pour chaque entrée mise à jour.

Vous êtes autorisé à planifier le redémarrage.

Étape 1 Accédez à **Network** > **Identification Service Engine** (Réseau > Network Identification Service Engine).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez la case **Enable ISE service** (Activer le service ISE).

Étape 4 Cochez la case **Enable** (Activer) pour permettre à Secure Web Appliance de récupérer les rubriques de liaison SXP des services ISE.

Par défaut, le service ISE SGT eXchange Protocol (SXP) est désactivé.

Étape 5 Cliquez sur **Start Test** (Démarrer le test) pour tester la connexion.

Remarque Les informations SXP ne s'affichent que si le service ISE-SGT eXchange Protocol (SXP) a été activé.

Étape 6 Cliquez sur **Submit** (Soumettre).

Vérification de la configuration du protocole ISE-SXP

Vous pouvez vérifier la configuration du protocole ISE-SXP en utilisant l'une des méthodes suivantes :

- Cliquez sur **Start Test** (Démarrer le test) dans le champ Activation du protocole ISE-SXP pour le mappage des adresses SGT vers les adresses IP, à la page 186 et vérifiez les informations affichées.
- Utilisez la commande **STATISTICS** sous la commande **ISEDATA** dans l'interface de ligne de commande AsyncOS (CLI).

Lorsque vous utilisez la commande **STATISTICS**, les informations suivantes s'affichent :

- Nom d'hôte ERS
- Heure de connexion ERS
- Téléchargement en bloc de session
- Téléchargement en bloc de groupe
- Téléchargement en bloc de SGT
- Téléchargement en bloc de SXP

- Mise à jour de la session
- Mise à jour de groupe
- Mise à jour SXP
- attribution de mémoire
- Désaffectation de mémoire
- Nombre total de sessions

Le nom d'utilisateur est généré dans le format suivant :

```
isesxp_<ISE-node-ip>_sgt<SGT number>_<Client IP address>
```

Par exemple : isesxp_10.10.2.68_sgt18_10.10.10.10

Authentification des utilisateurs VDI (Virtual Desktop Infrastructure) dans les intégrations ISE/ISE-PIC

Vous pouvez configurer une identification transparente avec ISE/ISE-PIC pour les utilisateurs dans des environnements VDI en fonction des ports source utilisés.

Vous devez installer l'agent Cisco Terminal Services (TS Agent) sur les serveurs VDI. L'agent Cisco TS fournit les renseignements d'identité à ISE/ISE-PIC. Les informations d'identité comprennent le domaine, le nom d'utilisateur et les plages de ports utilisées par chaque utilisateur.

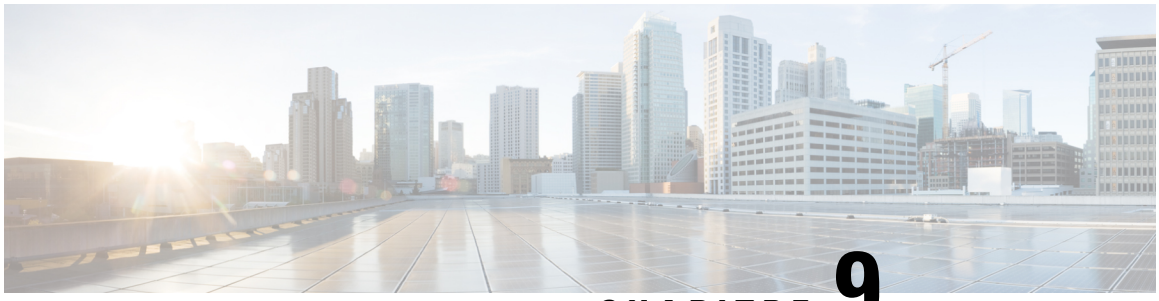
- Téléchargez Cisco TS agent à partir du site d'assistance https://www.cisco.com/c/en/us/support/index.html.
- Consultez le Guide de l'agent pour les services Cisco Terminal Services (TS) https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html pour en savoir plus.
- Configurez le fournisseur d'API ISE/ISE-PIC pour qu'il fonctionne avec un agent Cisco TS. Consultez la documentation sur les agents Cisco TS pour en savoir plus sur l'envoi d'appels d'API.

Remarque

- L'authentification de secours pour les utilisateurs de l'environnement VDI n'est pas prise en charge.
- Assurez-vous que le nombre maximal de sessions de bureau à distance est le même dans les paramètres d'agent de Cisco Terminal Services et du serveur Microsoft. Cela empêche l'envoi d'informations de session incorrectes à Secure Web Appliance par ISE et permet d'éviter les fausses authentifications pour les nouvelles sessions.

Résolution des problèmes du service Cisco de vérification des identités

- Problèmes liés au service Cisco de vérification des identités, on page 644



CHAPITRE 9

Classifier les URL pour l'application de la politique

Cette rubrique contient les sections suivantes :

Survol de la catégorisation des transactions URL

Les groupes de politiques vous permettent de créer des politiques sécurisées qui contrôlent l'accès aux sites Web au contenu douteux. Les sites bloqués, autorisés ou déchiffrés dépendent des catégories que vous sélectionnez lors de la configuration du blocage de catégories pour chaque groupe de politiques. Pour contrôler l'accès des utilisateurs en fonction d'une catégorie d'URL, vous devez activer les contrôles d'utilisation Web de Cisco. Il s'agit d'un moteur de filtrage d'URL multicouche qui utilise des préfixes de domaine et une analyse de mots-clés pour classer les URL.

Vous pouvez utiliser des catégories d'URL lors des tâches suivantes :

Option	Méthode
Définir l'appartenance à un groupe de politiques	Mise en correspondance des URL et des catégories d'URL, on page 193
Contrôler l'accès aux requêtes HTTP, HTTPS et FTP	Filtrage des transactions à l'aide de catégories d'URL, on page 202

Option	Méthode
Créer des catégories d'URL personnalisées définies par l'utilisateur qui précisent des noms d'hôte et des adresses IP spécifiques	Création et modification de catégories d'URL personnalisées, on page 211

Catégorisation des échecs de transactions URL

Le moteur Dynamic Content Analysis classe les URL lorsqu'il contrôle l'accès aux sites Web dans les politiques d'accès uniquement. Il ne catégorise pas les URL lors de la détermination de l'appartenance au groupe de politiques ou du contrôle de l'accès aux sites Web à l'aide des politiques de déchiffrement ou de sécurité des données Cisco. En effet, le moteur fonctionne en analysant le contenu de la réponse du serveur de destination. Il ne peut donc pas être utilisé pour les décisions qui doivent être prises au moment de la demande avant le téléchargement d'une réponse du serveur.

Si le score de réputation Web pour une URL non classée se trouve dans la plage WBRS ALLOW, AsyncOS autorise la demande sans effectuer d'analyse de contenu dynamique.

Une fois que le moteur d'analyse de contenu dynamique a catégorisé une URL, il stocke le verdict de la catégorie et l'URL dans une mémoire cache temporaire. Cela permet aux transactions futures de bénéficier de l'analyse de réponse précédente et d'être classées au moment de la demande plutôt qu'au moment de la réponse.

L'activation du moteur Dynamic Content Analysis peut avoir une incidence sur les performances des transactions. Cependant, la plupart des transactions sont classées à l'aide de la base de données de catégories d'URL Cisco Web Usage Controls. Par conséquent, le moteur Dynamic Content Analysis n'est généralement appelé que pour un faible pourcentage des transactions.

Activation du moteur Dynamic Content Analysis

Note Il est possible pour une politique d'accès, ou une identité utilisée dans une politique d'accès, de définir l'appartenance à la politique par une catégorie d'URL prédéfinie et que la politique d'accès effectue une action sur la même catégorie d'URL. L'URL dans la demande peut être non classée lors de la détermination de l'appartenance à un groupe de politiques d'identité et d'accès, mais elle doit être classée par le moteur Dynamic Content Analysis après avoir reçu la réponse du serveur. Cisco Web Usage Controls ignore le verdict de catégorie du moteur Dynamic Content Analysis et l'URL conserve le verdict « non classé » pour le reste de la transaction. Les transactions futures bénéficieront toujours du nouveau verdict de catégorie.

Étape 1 Choisissez **Security Services > Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable).

Étape 2 Activez Cisco Web Usage Controls.

Étape 3 **Cliquez** pour activer le moteur Dynamic Content Analysis.

Étape 4 Envoyez et validez les modifications.

URL non classées

Une URL non classée est une URL qui ne correspond à aucune catégorie d'URL prédéfinie ou à une catégorie d'URL personnalisée *incluse*.

Note Lors de la détermination de l'appartenance à un groupe de politiques, une catégorie d'URL personnalisée est considérée comme incluse, uniquement lorsqu'elle est sélectionnée pour l'appartenance au groupe de politiques.

Toutes les transactions donnant lieu à des catégories sans correspondance sont signalées dans la page Reporting > URL Categories (Rapports > Catégories d'URL) en tant que « URL non classées ». Un grand nombre d'URL non classées sont générées à partir de demandes adressées aux sites Web du réseau interne. Cisco recommande d'utiliser des catégories d'URL personnalisées pour regrouper les URL internes et autoriser toutes les demandes adressées aux sites Web internes. Cela diminue le nombre de transactions Web signalées comme « URL non classées » et signale plutôt les transactions internes dans les statistiques « URL Filtering Bypassed » (Filtrage d'URL contournés).

Thèmes connexes

- Interprétation des données non filtrées et non classées, on page 224.
- Création et modification de catégories d'URL personnalisées, on page 211.

Mise en correspondance des URL et des catégories d'URL

Lorsque le moteur de filtrage d'URL fait correspondre une catégorie d'URL à l'URL dans une demande de client, il évalue d'abord l'URL par rapport aux catégories d'URL personnalisées *incluses* dans le groupe de politiques. Si l'URL dans la demande ne correspond à aucune catégorie personnalisée incluse, le moteur de filtrage d'URL la compare aux catégories d'URL prédéfinies. Si l'URL ne correspond à aucune catégorie d'URL personnalisée ou prédéfinie incluse, la demande est non classée.

Note Lors de la détermination de l'appartenance à un groupe de politiques, une catégorie d'URL personnalisée est considérée comme incluse uniquement lorsqu'elle est sélectionnée pour l'appartenance à un groupe de politiques.

Pour voir à quelle catégorie un site Web en particulier est affecté, accédez à l'URL dans Signalisation des URL non classées et mal classées, on page 193.

Thèmes connexes

- URL non classées, on page 193.

Signalisation des URL non classées et mal classées

Vous pouvez signaler à Cisco des URL non classées et mal classées. Cisco fournit un outil d'envoi d'URL sur son site Web qui vous permet d'envoyer plusieurs URL simultanément :

- https://talosintelligence.com/tickets

- Pour vérifier l'état des URL envoyées, cliquez sur l'onglet Status on Submitted URLs (État des URL envoyées) sur cette page.
- Vous pouvez également utiliser l'outil d'envoi d'URL pour rechercher la catégorie d'URL attribuée pour n'importe quelle URL.

- https://www.talosintelligence.com/reputation_center/support
  - Pour envoyer une contestation, vous devez être connecté à votre compte Cisco. Les conflits peuvent être signalés pour des URL, des adresses IP ou des domaines.
  - Utilisez la zone de recherche du centre de réputation pour rechercher des informations de réputation Web.

Base de données des catégories d'URL

La catégorie dans laquelle se trouve une URL est déterminée par une base de données de catégories de filtrage. Secure Web Appliance recueille des informations et gère une base de données distincte pour chaque moteur de filtrage d'URL. Les bases de données des catégories de filtrage reçoivent régulièrement des mises à jour du serveur de mise à jour Cisco.

La base de données des catégories d'URL comprend de nombreux facteurs et sources de données internes à Cisco et provenant d'Internet. L'un des facteurs occasionnellement pris en compte, et fortement modifié par rapport à l'origine, est l'information du projet Open Directory.

Pour voir à quelle catégorie un site Web en particulier est affecté, accédez à l'URL dans Signalisation des URL non classées et mal classées, on page 193.

Thèmes connexes

- Mise à jour manuelle de l'ensemble de catégories d'URL , on page 200

Configuration du moteur de filtrage d'URL

Par défaut, le moteur de filtrage d'URL Cisco Web Usage Controls est activé dans l'Assistant de configuration du système.

Étape 1 Choisissez **Security Services > Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Vérifiez que la propriété Enable Acceptable Use Controls (Activer les contrôles d'utilisation acceptable) est activée.

Étape 4 Choisissez l'un des contrôles d'utilisation du Web Cisco suivants :

a. Application Visibility and Control (Visibilité et contrôle des applications)

b. Dynamic Content Analysis Engine (Moteur Dynamic Content Analysis)

c. Multiple URL Categories (Catégories d'URL multiples)

Note La fonctionnalité Multiple URL Categories (Catégories d'URL multiples) s'applique uniquement aux politiques d'accès. Vous ne pouvez pas appliquer la fonctionnalité Multiple URL Categories (Catégories d'URL multiples) aux politiques de déchiffrement et aux profils d'identification.

Note La fonctionnalité Multiple URL Categories (Catégories d'URL multiples) ne s'applique qu'aux catégories prédéfinies et non aux catégories personnalisées.

L'activation de cette option entraîne la modification des catégories Web liées aux politiques d'accès. Autrement dit, si une configuration est effectuée avec une URL ayant au moins deux catégories prédéfinies, une condition OU est appliquée parmi les différentes catégories d'URL. Ainsi, l'action de la politique d'accès (BLOCK, MONITOR ou WARN) sera déterminée en fonction du résultat de la condition OU collective.

Par exemple, imaginons que vous ayez une URL avec xyz.com et que le réseau ait trois catégories d'URL différentes, A, B et C. Si vous avez configuré les états A comme MONITOR, B comme BLOCK et C comme WARN, une opération OU collective renverrait BLOCK pour la transaction.

	Catégorie d'URL A	**Catégorie d'URL B**	**Catégorie d'URL C**	**Action globale de la condition OU**
xyz.com	MONITEUR	BLOQUER	WARN	BLOQUER
abc.com	MONITEUR	MONITEUR	WARN	WARN
def.com	MONITEUR	MONITEUR	MONITEUR	MONITEUR

Lorsque la fonctionnalité Multiple URL Categories (Catégories d'URL multiples) est désactivée, seule la catégorie principale (la première) est prise en compte. L'action de la politique d'accès sera basée sur la configuration de la catégorie principale uniquement.

Étape 5 Choisissez l'action par défaut que le proxy Web doit utiliser lorsque le moteur de filtrage d'URL n'est pas disponible, soit Monitor (Superviser) ou Block (Bloquer). La valeur par défaut est Monitor (Superviser).

Étape 6 Envoyez et validez les modifications.

Gestion des mises à jour de l'ensemble de catégories d'URL

L'ensemble de catégories d'URL prédéfinies peut à l'occasion être mis à jour afin de l'adapter aux nouvelles tendances Web et aux modèles d'utilisation en constante évolution. Les mises à jour de l'ensemble de catégories d'URL sont distinctes des modifications qui ajoutent de nouvelles URL et remappent les URL mal classées. Les mises à jour d'ensembles de catégories peuvent modifier les configurations de vos politiques existantes et, par conséquent, nécessiter une action. Des mises à jour d'ensembles de catégories d'URL peuvent se produire entre les versions du produit; il n'est pas nécessaire de mettre à niveau AsyncOS.

Des informations sont disponibles à l'adresse : http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html.

Effectuez les actions suivantes :

Quand agir	Méthode
Avant les mises à jour (Effectuez ces tâches lors de la configuration initiale)	Interprétation des impacts des mises à jour de l'ensemble de catégories d'URL , on page 196 Contrôle des mises à jour de l'ensemble de catégories d'URL , on page 200 Paramètres par défaut pour les catégories nouvelles et modifiées , on page 200 Réception d'alertes concernant les modifications apportées aux catégories et aux politiques , on page 201
Après les mises à jour	Réponse aux alertes concernant les mises à jour d'ensembles de catégories d'URL , on page 201

Interprétation des impacts des mises à jour de l'ensemble de catégories d'URL

Les mises à jour des ensembles de catégories d'URL peuvent avoir les incidences suivantes sur les politiques d'accès, les politiques de déchiffrement, les politiques de sécurité des données de Cisco, ainsi que sur les identités :

- Effets des modifications apportées à l'ensemble de catégories d'URL sur l'appartenance au groupe de politiques , on page 196
- Effets des mises à jour de l'ensemble de catégories d'URL sur les actions de filtrage dans les politiques , on page 196

Effets des modifications apportées à l'ensemble de catégories d'URL sur l'appartenance au groupe de politiques

Cette section s'applique à tous les types de politiques dont l'appartenance peut être définie par catégorie d'URL, ainsi qu'aux identités. Lorsque l'appartenance à un groupe de politiques est définie par catégorie d'URL, les modifications apportées à l'ensemble de catégories peuvent avoir les effets suivants :

- Si le seul critère d'appartenance est une catégorie supprimée, la politique ou l'identité est désactivée.

Si l'appartenance à une politique est définie par une catégorie d'URL qui change, et si cela entraîne des modifications de la liste d'ACL, le proxy Web redémarrera.

Effets des mises à jour de l'ensemble de catégories d'URL sur les actions de filtrage dans les politiques

Les mises à jour des ensembles de catégories d'URL peuvent modifier le comportement des politiques des façons suivantes :

Modification	Effet sur les politiques et les identités
Une nouvelle catégorie peut être ajoutée	Pour les nouvelles catégories d'URL, l'une des actions suivantes sera sélectionnée dans l'option Default Action for Update Categories (Action par défaut pour les catégories de mise à jour) dans la page de configuration des politiques : • Least Restrictive (Le moins restrictif) • Most Restrictive (Le plus restrictif) Les actions sont définies par défaut pour les nouvelles catégories. Dans Access Policies (Politiques d'accès) et Cisco Data Security Policies (Politiques de sécurité des données de Cisco) : • Le plus restrictif est Block (Bloquer) • Le moins restrictif est Monitor (Superviser) Dans les politiques de dérivation du trafic Web (WTT) : • Le plus restrictif est Tap (Dérivation) • Le moins restrictif est No Tap (Sans dérivation) Dans Decryption Policies (Politiques de déchiffrement) : • Le plus restrictif est Block (Bloquer) • Le moins restrictif est Pass Through (Intercommunication)
Une catégorie peut être supprimée	L'action associée à la catégorie supprimée est supprimée. Si la politique dépend exclusivement de la catégorie supprimée, elle est désactivée. Si une politique dépend d'une identité qui dépendait exclusivement d'une catégorie supprimée, la politique sera désactivée.
Une catégorie peut être renommée	Aucun changement de comportement de la politique existante.
Une catégorie peut être fractionnée	Une seule catégorie peut servir à créer plusieurs nouvelles catégories. Les actions des nouvelles catégories seront sélectionnées dans l'action par défaut pour les catégories de mise à jour.

Modification	Effet sur les politiques et les identités
Deux catégories existantes ou plus peuvent fusionner	Si la même action est affectée à toutes les catégories d'origine d'une politique, la catégorie fusionnée a la même action que les catégories d'origine. Si toutes les catégories d'origine étaient définies sur « Use Global Setting » (Utiliser les paramètres globaux), la catégorie fusionnée est également définie sur « Use Global Setting » (Utiliser les paramètres globaux). Si la politique avait différentes actions attribuées aux catégories d'origine, l'action attribuée à la catégorie fusionnée dépend du paramètre d'URL non classées de cette politique : • Si l'option Uncategorized URLs (URL non classées) est Block (Bloquer) [ou « Use Global Setting » (Utiliser le paramètre global) si le paramètre global est Block (Bloquer)], l'action la plus restrictive parmi les catégories d'origine est appliquée à la catégorie fusionnée. • Si l'option Uncategorized URLs (URL non classées) est définie sur une action autre que Block (Bloquer) ou [« Use Global Setting » (Utiliser le paramètre global)], l'action la moins restrictive parmi les catégories d'origine est appliquée à la catégorie fusionnée. Dans ce cas, les sites qui étaient auparavant bloqués peuvent désormais être accessibles aux utilisateurs. Si l'appartenance à la politique est définie par une catégorie d'URL et que certaines des catégories concernées par la fusion, ou l'action Uncategorized URLs (URL non classées), ne sont pas incluses dans la définition de l'appartenance à la politique, les valeurs de la politique globale sont utilisées pour les éléments manquants. L'ordre de restriction est le suivant (toutes les actions ne sont pas disponibles pour tous les types de politiques) : • Block (Bloquer) • Abandonner • Déchiffrer • Avertir • Basé sur le temps • Monitor (Surperviser) • Intercommunication **Note** Les politiques basées sur le temps qui reposent sur des catégories fusionnées adoptent l'action associée à l'une des catégories d'origine. (Il est possible que les politiques basées sur le temps ne comprennent pas d'action manifestement la plus restrictive ou la moins restrictive.)

Thèmes connexes

- Catégories fusionnées - Exemples , on page 199.

Catégories fusionnées - Exemples

Quelques exemples de catégories fusionnées, en fonction des paramètres de la page de filtrage d'URL pour la politique :

Catégorie d'origine 1	Catégorie d'origine 2	URL non classées	Catégorie fusionnée
Monitor (Surperviser)	Monitor (Surperviser)	(Sans objet)	Monitor (Surperviser)
Block (Bloquer)	Block (Bloquer)	(Sans objet)	Block (Bloquer)
Utiliser les paramètres globaux	Utiliser les paramètres globaux	(Sans objet)	Utiliser les paramètres globaux
Avertir	Block (Bloquer)	Monitor (Surperviser) Utilisez la catégorie la moins restrictive parmi les catégories initiales.	Avertir
Monitor (Surperviser)	• Bloquer ou • Utiliser les paramètres globaux lorsque Global est réglé sur Block (Bloquer)	• Bloquer ou • Utiliser le paramètre global lorsque Global est réglé sur Block (Bloquer) Utilisez la catégorie la plus restrictive parmi les catégories initiales.	Block (Bloquer)
Block (Bloquer)	• Monitor (Superviser) ou • Utiliser les paramètres globaux, lorsque Global est réglé sur Monitor (Superviser)	• Monitor (Superviser) ou • Utiliser le paramètre global lorsque Global est réglé sur Monitor (Superviser) Utilisez la catégorie la moins restrictive parmi les catégories initiales.	Monitor (Surperviser)
Pour les politiques dans lesquelles l'appartenance est définie par catégorie d'URL : Monitor (Surperviser)	Aucune action pour cette catégorie n'est spécifiée dans cette politique, mais la valeur dans la politique globale de cette catégorie est Block (Bloquer)	Aucune action pour les URL non classées n'est spécifiée dans cette politique, mais la valeur dans la politique globale pour les URL non classées est Monitor (Superviser).	Monitor (Surperviser)

Contrôle des mises à jour de l'ensemble de catégories d'URL

Par défaut, les mises à jour des catégories d'URL s'effectuent automatiquement. Ces mises à jour peuvent modifier les configurations de politiques existantes. Vous pouvez donc choisir de désactiver toutes les mises à jour automatiques.

Option	Méthode
Si vous désactivez les mises à jour, vous devrez mettre à jour manuellement tous les services répertoriés dans la section Update Servers (list) [Serveurs de mise à jour (liste)] de la page System Administration > Upgrade and Update Settings (Administration système > Paramètres de mise à jour et de mise à niveau).	Mise à jour manuelle de l'ensemble de catégories d'URL , on page 200 et Mise à jour manuelle des composants du service Security, on page 616
Désactivation de toutes les mises à jour automatiques	Configuration des paramètres de mise à niveau et de mise à jour de services, on page 619.

Note Si vous utilisez l'interface de ligne de commande, désactivez les mises à jour en réglant l'intervalle de mise à jour sur zéro (0)

Mise à jour manuelle de l'ensemble de catégories d'URL

Note

- N'interrompez pas une mise à jour en cours.
- Si vous avez désactivé les mises à jour automatiques, vous pouvez mettre à jour manuellement l'ensemble de catégories d'URL à votre gré.

Étape 1 Choisissez **Security Services > Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable).

Étape 2 Déterminez si une mise à jour est disponible :

Examinez l'élément « Cisco Web Usage Controls - Web Categorization Categories List » (Cisco Web Usage Controls - Liste des catégories de catégorisation Web) dans le tableau des mises à jour du moteur Acceptable Use Controls.

Étape 3 Pour effectuer la mise à jour, cliquez sur **Update Now** (Mettre à jour maintenant).

Paramètres par défaut pour les catégories nouvelles et modifiées

Les mises à jour des catégories d'URL peuvent modifier le comportement de vos politiques existantes. Vous devez préciser les paramètres par défaut de certaines modifications lorsque vous configurez vos politiques, afin qu'elles soient prêtes lorsque des mises à jour d'ensembles de catégories d'URL se produisent. Lorsque de nouvelles catégories sont ajoutées ou que des catégories existantes fusionnent dans une nouvelle catégorie,

l'action par défaut pour ces catégories pour chaque politique est affectée par le paramètre **Default Action for Update Categories** (Action par défaut pour la mise à jour des catégories) de cette politique.

Vérification des paramètres existants ou modification des paramètres

Étape 1 Choisissez **Web Security Manager**.

Étape 2 Pour chaque politique d'accès, politique de déchiffrement et politique de sécurité des données de Cisco, cliquez sur le lien **URL Filtering** (Filtrage d'URL).

Étape 3 Vérifiez le paramètre sélectionné pour les URL non classées.

What to do next

Thèmes connexes

- Effets des mises à jour de l'ensemble de catégories d'URL sur les actions de filtrage dans les politiques , on page 196.

Réception d'alertes concernant les modifications apportées aux catégories et aux politiques

Les mises à jour de l'ensemble de catégories déclenchent deux types d'alertes :

- Alertes concernant les changements de catégorie
- Alertes sur les politiques qui ont été modifiées ou désactivées à la suite de modifications d'ensembles de catégories.

Étape 1 Choisissez **System Administration > Alerts** (Administration système > Alertes).

Étape 2 Cliquez sur **Add Recipient** (Ajouter un destinataire) et ajoutez une adresse de messagerie (ou plusieurs adresses de messagerie).

Étape 3 Décidez quels **types d'alerte** et quelles **gravités d'alerte** recevoir.

Étape 4 Envoyez et validez les modifications.

Réponse aux alertes concernant les mises à jour d'ensembles de catégories d'URL

Lorsque vous recevez une alerte concernant des modifications de l'ensemble de catégories, procédez comme suit :

- Vérifiez les politiques et les identités pour vous assurer qu'ils atteignent toujours vos objectifs de politique après les fusions, les ajouts et les suppressions de catégories, et
- Envisagez de modifier les politiques et les identités pour bénéficier des nouvelles catégories et de la granularité supplémentaire des catégories fractionnées.

Thèmes connexes

- Interprétation des impacts des mises à jour de l'ensemble de catégories d'URL , on page 196

Filtrage des transactions à l'aide de catégories d'URL

Le moteur de filtrage d'URL vous permet de filtrer les transactions dans les politiques d'accès, de déchiffrement et de sécurité des données. Lorsque vous configurez des catégories d'URL pour les groupes de politiques, vous pouvez configurer des actions pour les catégories d'URL personnalisées, le cas échéant, et les catégories d'URL prédéfinies.

Les actions de filtrage d'URL que vous pouvez configurer dépendent du type de groupe de politiques :

Option	Méthode
Politiques d'accès	Configuration des filtres d'URL pour les groupes de politiques d'accès, on page 202
Politiques de déchiffrement	Configuration des filtres d'URL pour les groupes de politiques de déchiffrement, on page 205
Politiques de sécurité des données de Cisco	Configuration des filtres d'URL pour les groupes de politiques de sécurité des données, on page 207

Thèmes connexes

- Redirection du trafic dans les politiques d'accès, on page 221
- Aviser les utilisateurs et leur permettre de continuer, on page 222
- Création et modification de catégories d'URL personnalisées, on page 211
- Effets des mises à jour de l'ensemble de catégories d'URL sur les actions de filtrage dans les politiques , on page 196

Configuration des filtres d'URL pour les groupes de politiques d'accès

Vous pouvez configurer le filtrage d'URL pour les groupes de politiques d'accès définis par l'utilisateur et le groupe de politiques global.

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans le tableau des politiques, sous la colonne URL Filtering (Filtrage d'URL), pour le groupe de politiques que vous souhaitez modifier.

Étape 3 (Facultatif) Dans la section Custom URL Category Filtering (Filtrage des catégories d'URL personnalisées), vous pouvez ajouter des catégories d'URL personnalisées sur lesquelles effectuer une action dans cette politique :

a) Cliquez sur **Select Custom Categories** (Sélectionner des catégories personnalisées).

b) Choisissez les catégories d'URL personnalisées à inclure dans cette politique et cliquez sur **Apply** (Appliquer).

Choisissez les catégories d'URL personnalisées auxquelles le moteur de filtrage d'URL doit comparer la demande du client. Le moteur de filtrage d'URL compare les demandes des clients aux catégories d'URL personnalisées incluses et ignore les catégories d'URL personnalisées exclues. Le moteur de filtrage d'URL compare l'URL dans une demande d'un client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la politique apparaissent dans la section Custom URL Category Filtering (Filtrage de catégories d'URL personnalisées).

Étape 4 Dans la section Custom URL Category Filtering (Filtrage de catégorie d'URL personnalisée), choisissez une action pour chaque catégorie d'URL personnalisée incluse.

Action	Description
Utiliser les paramètres globaux	Utilise l'action pour cette catégorie dans le groupe de politiques globales. Il s'agit de l'action par défaut pour les groupes de politiques définies par l'utilisateur. S'applique uniquement aux groupes de politiques définies par l'utilisateur. **Note** Lorsqu'une catégorie d'URL personnalisée est exclue de la politique d'accès globale, l'action par défaut pour les catégories d'URL personnalisées incluses dans les politiques d'accès définies par l'utilisateur est Monitor (Superviser) au lieu de l'option Use Global Settings (Utiliser les paramètres globaux). Vous ne pouvez pas choisir Use Global Settings (Utiliser les paramètres globaux) lorsqu'une catégorie d'URL personnalisée est exclue de la politique d'accès globale.
Block (Bloquer)	Le proxy Web refuse les transactions qui correspondent à ce paramètre.
Rediriger	Redirige le trafic destiné à l'origine à une URL dans cette catégorie vers un emplacement que vous spécifiez. Lorsque vous choisissez cette action, le champ Redirect to (Rediriger vers) s'affiche. Entrez une URL vers laquelle rediriger tout le trafic.
Allow (Autoriser)	Toujours autoriser les demandes des clients pour les sites Web de cette catégorie. Les demandes autorisées contournent tout filtrage supplémentaire et analyse les programmes malveillants. Utilisez ce paramètre uniquement pour les sites Web approuvés. Vous pourriez souhaiter utiliser ce paramètre pour les sites internes.
Monitor (Surperviser)	Le proxy Web n'autorise ni ne bloque la demande. Au lieu de cela, il continue à évaluer la demande du client en fonction d'autres paramètres de contrôle de groupe de politiques, tels que le filtrage de réputation Web.
Avertir	Le proxy Web bloque dans un premier temps la demande et affiche une page d'avertissement, mais permet à l'utilisateur de continuer en cliquant sur un lien hypertexte dans la page d'avertissement.
Basé sur les quotas	Lorsqu'un utilisateur individuel s'approche du quota de volume ou de temps que vous avez spécifié, un avertissement s'affiche. Lorsqu'un quota est atteint, une page de blocage s'affiche. Consultez Plages de temps et quotas, on page 269.
Basé sur le temps	Le proxy Web bloque ou surveille la demande pendant les plages de temps que vous définissez. Consultez Plages de temps et quotas, on page 269.

Étape 5 Dans la section Predefined URL Category Filtering (Filtrage de catégories d'URL prédéfinies), choisissez l'une des actions suivantes pour chaque catégorie :

- Utiliser les paramètres globaux
- Monitor (Surperviser)

- Avertir
- Block (Bloquer)
- Basé sur le temps
- Basé sur les quotas

Étape 6 Dans la section Uncategorized URLs (URL non classées), choisissez l'action à entreprendre pour les demandes des clients adressées aux sites Web qui n'entrent pas dans une catégorie d'URL prédéfinie ou personnalisée. Ce paramètre détermine également l'action par défaut pour les catégories nouvelles et fusionnées résultant des mises à jour de l'ensemble de catégories d'URL.

Étape 7 Envoyez et validez les modifications.

What to do next

- Exceptions au blocage pour le contenu intégré et référencé, on page 204

Exceptions au blocage pour le contenu intégré et référencé

Un site Web peut intégrer ou faire référence à du contenu classé différemment de la page source ou qui est considéré comme une application. Par défaut, le contenu intégré/référencé est bloqué ou surveillé en fonction de l'action sélectionnée pour la catégorie ou l'application qui lui est attribuée, quel que soit la classification du site Web source. Par exemple, un site Web d'*actualité* peut contenir du contenu classé comme *diffusion en continu de vidéos* et identifié comme étant l'application YouTube. Selon votre politique, la *diffusion en continu de vidéo* et YouTube sont tous deux bloqués, tandis que les sites d'*actualités* ne le sont pas.

Note Les demandes de contenu intégré comprennent généralement l'adresse du site d'où provient la demande (c'est ce que l'on appelle le champ « referer » (référent) dans l'en-tête HTTP de la demande). Ces informations d'en-tête sont utilisées pour déterminer la classification du contenu référencé.

Vous pouvez utiliser cette fonctionnalité pour définir des exceptions aux actions par défaut pour le contenu intégré ou recommandé; par exemple, pour autoriser tout contenu intégré ou référencé à partir de sites Web d'*actualités* ou d'une catégorie personnalisée représentant votre intranet.

Note Les exceptions basées sur les référents sont prises en charge uniquement dans les politiques d'accès. Pour utiliser cette fonctionnalité avec le trafic HTTPS, avant de définir des exceptions dans les politiques d'accès, vous devez configurer le déchiffrement HTTPS des catégories d'URL que vous sélectionnerez pour les exceptions. Consultez Configuration des filtres d'URL pour les groupes de politiques de déchiffrement, on page 205 pour obtenir des informations sur la configuration du déchiffrement HTTPS. Consultez Conditions et restrictions des exceptions au blocage pour le contenu intégré et le contenu mentionné, on page 643 pour en savoir plus sur l'utilisation de cette fonctionnalité avec le déchiffrement HTTPS.

Étape 1 Dans la page de filtrage d'URL d'une politique d'accès particulière (voir Configuration des filtres d'URL pour les groupes de politiques d'accès, on page 202, cliquez sur **Enable Exceptions** (Activer les exceptions) dans la section Exceptions to Blocking for Embedded/Referred Content (Exceptions au blocage pour le contenu intégré/référencé).

Étape 2 Cliquez sur le lien **Click to select categories** (Cliquer pour sélectionner des catégories) dans la colonne Set Exception for Content Referred by These Categories (Définir une exception pour le contenu référencé par ces catégories) afin d'afficher la page de sélection d'une exception de référence de catégorie de filtrage d'URL.

Étape 3 Dans les listes d'URL prédéfinies et personnalisées, sélectionnez les catégories pour lesquelles vous souhaitez définir cette exception de recommandation, puis cliquez sur **Done** (Terminé) afin de revenir à la page de filtrage d'URL pour cette politique d'accès.

Étape 4 Choisissez un type d'exception dans la liste déroulante Set Exception for this Referred Content (Définir une exception pour ce contenu référencé) :

- **All embedded/referred content** (Tout le contenu intégré ou référencé) : tout contenu intégré dans des sites des types de catégories précisés ou référencé à partir de ces sites n'est pas bloqué, quelle que soit la classification de ce contenu.
- **Selected embedded/referred content** (Contenu intégré ou référencé sélectionné) : après avoir choisi cette option, sélectionnez des catégories et des applications spécifiques qui ne sont pas bloquées lorsqu'elles proviennent des catégories d'URL spécifiées.
- **All embedded/referred content except** (Tout le contenu intégré/référencé, excepté) : après avoir choisi cette option, tout le contenu intégré dans les sites des types de catégories précisés et provenant de ceux-ci n'est pas bloqué, à l'exception des catégories d'URL et des applications que vous spécifiez maintenant ici. Autrement dit, ces types resteront bloqués.

Note L'option Referrer Exception (Exception de référent) est activée par défaut pour la catégorie d'URL personnalisée même lorsque cette catégorie n'est pas incluse dans les politiques d'accès.

Étape 5 Envoyez et validez les modifications.

What to do next

Vous pouvez choisir d'afficher les données de transaction de l'autorisation dans les tableaux et les graphiques fournis dans les pages de Rapports suivantes : catégories d'URL, utilisateurs et sites Web, ainsi que les tableaux connexes dans la page de survol. Consultez Choix des données à représenter au format graphique , on page 403 pour en savoir plus sur la sélection des options d'affichage de la carte.

Configuration des filtres d'URL pour les groupes de politiques de déchiffrement

Vous pouvez configurer le filtrage d'URL pour les groupes de politiques de déchiffrement définis par l'utilisateur et le groupe de politiques de déchiffrement globale.

Étape 1 Choisissez **Web Security Manager > Decryption Policies** (Web Security Manager > Politiques de déchiffrement).

Étape 2 Cliquez sur le lien dans le tableau des politiques, sous la colonne URL Filtering (Filtrage d'URL), pour le groupe de politiques que vous souhaitez modifier.

Étape 3 (Facultatif) Dans la section Custom URL Category Filtering (Filtrage des catégories d'URL personnalisées), vous pouvez ajouter des catégories d'URL personnalisées sur lesquelles effectuer une action dans cette politique :

a) Cliquez sur **Select Custom Categories** (Sélectionner des catégories personnalisées).
b) Choisissez les catégories d'URL personnalisées à inclure dans cette politique et cliquez sur **Apply** (Appliquer).

Choisissez les catégories d'URL personnalisées auxquelles le moteur de filtrage d'URL doit comparer la demande du client. Le moteur de filtrage d'URL compare les demandes des clients aux catégories d'URL personnalisées incluses et ignore les catégories d'URL personnalisées exclues. Le moteur de filtrage d'URL compare l'URL dans une demande d'un client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la politique apparaissent dans la section Custom URL Category Filtering (Filtrage de catégories d'URL personnalisées).

Étape 4 Choisissez une action pour chaque catégorie d'URL personnalisée et prédéfinie.

Action	Description
Utiliser les paramètres globaux	Utilise l'action pour cette catégorie dans le groupe global de politiques de déchiffrement. Il s'agit de l'action par défaut pour les groupes de politiques définies par l'utilisateur. S'applique uniquement aux groupes de politiques définies par l'utilisateur. Lorsqu'une catégorie d'URL personnalisée est exclue de la politique de déchiffrement globale, l'action par défaut pour les catégories d'URL personnalisées incluses dans les politiques de déchiffrement définies par l'utilisateur est Surperviser au lieu d'utiliser les paramètres globaux. Vous ne pouvez pas choisir Use Global Settings (Utiliser les paramètres globaux) lorsqu'une catégorie d'URL personnalisée est exclue de la politique de déchiffrement globale.
Intercommunication	Transmet la connexion entre le client et le serveur sans inspecter le contenu du trafic.
Monitor (Surperviser)	Le proxy Web n'autorise ni ne bloque la demande. Au lieu de cela, il continue à évaluer la demande du client en fonction d'autres paramètres de contrôle de groupe de politiques, tels que le filtrage de réputation Web.
Déchiffrer	Autorise la connexion, mais inspecte le contenu du trafic. L'appliance déchiffre le trafic et applique des politiques d'accès au trafic déchiffré comme s'il s'agissait d'une connexion HTTP en texte brut. En déchiffrant la connexion et en appliquant des politiques d'accès, vous pouvez analyser le trafic à la recherche de programmes malveillants.
Abandonner	Abandonne la connexion et ne transmet pas la demande de connexion au serveur. L'appliance n'informe pas l'utilisateur qu'il a abandonné la connexion.

Note Si vous souhaitez *bloquer* une catégorie d'URL particulière pour les demandes HTTPS, choisissez de déchiffrer cette catégorie d'URL dans le groupe de politique de déchiffrement, puis choisissez de bloquer la même catégorie d'URL dans le groupe de politique d'accès.

Étape 5 Dans la section Uncategorized URLs (URL non classées), choisissez l'action à entreprendre pour les demandes des clients adressées aux sites Web qui n'entrent pas dans une catégorie d'URL prédéfinie ou personnalisée.

Ce paramètre détermine également l'action par défaut pour les catégories nouvelles et fusionnées résultant des mises à jour de l'ensemble de catégories d'URL.

Étape 6 Envoyez et validez les modifications.

Configuration des filtres d'URL pour les groupes de politiques de sécurité des données

Vous pouvez configurer le filtrage d'URL pour les groupes de politiques de sécurité des données définis par l'utilisateur et le groupe de politiques globales.

Étape 1 Choisissez **Web Security Manager > Cisco Data Security** (Web Security Manager > Politiques de sécurité des données de Cisco).

Étape 2 Cliquez sur le lien dans le tableau des politiques, sous la colonne URL Filtering (Filtrage d'URL), pour le groupe de politiques que vous souhaitez modifier.

Étape 3 (Facultatif) Dans la section Custom URL Category Filtering (Filtrage des catégories d'URL personnalisées), vous pouvez ajouter des catégories d'URL personnalisées sur lesquelles effectuer une action dans cette politique :

a) Cliquez sur **Select Custom Categories** (Sélectionner des catégories personnalisées).

b) Choisissez les catégories d'URL personnalisées à inclure dans cette politique et cliquez sur **Apply** (Appliquer).

Choisissez les catégories d'URL personnalisées auxquelles le moteur de filtrage d'URL doit comparer la demande du client. Le moteur de filtrage d'URL compare les demandes des clients aux catégories d'URL personnalisées incluses et ignore les catégories d'URL personnalisées exclues. Le moteur de filtrage d'URL compare l'URL dans une demande d'un client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la politique apparaissent dans la section Custom URL Category Filtering (Filtrage de catégories d'URL personnalisées).

Étape 4 Dans la section Custom URL Category Filtering (Filtrage de catégories d'URL personnalisées), choisissez une action pour chaque catégorie d'URL personnalisée.

Action	Description
Utiliser les paramètres globaux	Utilise l'action pour cette catégorie dans le groupe de politiques globales. Il s'agit de l'action par défaut pour les groupes de politiques définies par l'utilisateur. S'applique uniquement aux groupes de politiques définies par l'utilisateur. Lorsqu'une catégorie d'URL personnalisée est exclue de la politique de sécurité des données de Cisco globale, l'action par défaut pour les catégories d'URL personnalisées incluses dans les politiques de sécurité des données de Cisco définies par l'utilisateur est Monitor (Superviser) au lieu de Use Global Settings (Utiliser les paramètres globaux). Vous ne pouvez pas choisir Use Global Settings (Utiliser les paramètres globaux) si une catégorie d'URL personnalisée est exclue de la politique de sécurité des données globale de Cisco.
Allow (Autoriser)	Toujours autoriser les demandes de téléchargement pour les sites Web de cette catégorie. S'applique uniquement aux catégories d'URL personnalisées. Les demandes autorisées contournent toutes les autres analyses de sécurité des données et la demande est évaluée par rapport aux politiques d'accès. Utilisez ce paramètre uniquement pour les sites Web approuvés. Vous pourriez souhaiter utiliser ce paramètre pour les sites internes.
Monitor (Surperviser)	Le proxy Web n'autorise ni ne bloque la demande. Au lieu de cela, il continue à évaluer la demande de téléchargement en fonction d'autres paramètres de contrôle de groupe de politiques, tels que le filtrage de réputation de sites Web.

Action	Description
Block (Bloquer)	Le proxy Web refuse les transactions qui correspondent à ce paramètre.

Note Si vous ne désactivez pas la limite de taille de fichier maximale, Secure Web Appliance continue de valider la taille de fichier maximale lorsque les options Allow (Autoriser) ou Monitor (Superviser) sont sélectionnées dans le filtrage d'URL.

Étape 5 Dans la section Predefined URL Category Filtering (Filtrage de catégories d'URL prédéfinies), choisissez l'une des actions suivantes pour chaque catégorie :

- Utiliser les paramètres globaux
- Monitor (Surperviser)
- Block (Bloquer)

Étape 6 Dans la section des URL non classées, choisissez l'action à entreprendre pour les demandes de chargement sur des sites Web qui n'entrent pas dans une catégorie d'URL prédéfinie ou personnalisée. Ce paramètre détermine également l'action par défaut pour les catégories nouvelles et fusionnées résultant des mises à jour de l'ensemble de catégories d'URL.

Étape 7 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Effets des mises à jour de l'ensemble de catégories d'URL sur les actions de filtrage dans les politiques , on page 196.

Catégorisation YouTube

La fonction de catégorisation YouTube vous permet de créer une catégorie d'URL personnalisée pour YouTube et de définir des politiques sur la catégorie personnalisée YouTube pour un accès sécurisé et contrôlé.

Remarque Lorsque vous configurez les règles d'accès basé sur la durée pour bloquer une catégorie YouTube spécifique :

- Les règles basées sur le temps que vous définissez ne s'appliquent pas aux vidéos déjà ouvertes en cours au moment où vous configurez la politique d'accès.
- Les règles seront applicables uniquement aux vidéos qui sont nouvellement ouvertes après que vous ayez défini les règles.

Remarque

- Assurez-vous que googleapis.com n'est pas bloqué dans le proxy en amont ou dans le pare-feu en amont. Si vous avez configuré une exception pour le serveur de mise à jour Cisco et le serveur de télémesure WBNP, configurez la même pour googleapis.com également.
- Vous ne pouvez pas bloquer la vidéo qui s'affiche sur la page principale d'une chaîne, même si la vidéo appartient à une catégorie YouTube bloquée.

  Par exemple, vous avez bloqué des voitures et des véhicules dans la catégorie YouTube. Si vous ouvrez une vidéo dans la catégorie précisée sur la page principale d'une chaîne relative aux voitures et aux voitures, la vidéo ne sera pas bloquée. Si vous essayez d'ouvrir la même vidéo dans un onglet distinct, elle sera bloquée comme prévu.

Pour configurer la fonction de catégorisation YouToube, effectuez les tâches suivantes.

Étape	Tâche	Liens vers les rubriques et les procédures
1.	Créez une catégorie d'URL personnalisée et externe pour YouTube à l'aide de www.youtube.com et m.youtube.com.	Création et modification de catégories d'URL personnalisées, à la page 211.
2.	Ajouter une catégorie d'URL personnalisée et externe pour YouTube à une politique de déchiffrement.	Configuration des filtres d'URL pour les groupes de politiques de déchiffrement, à la page 205.
3.	Activez la fonction de catégorisation de YouTube.	Activation de la fonctionnalité de catégorisation de YouTube, à la page 209.
4.	Appliquez des politiques d'accès aux catégories d'URL personnalisées et externes pour YouTube.	Configuration des filtres d'URL pour les groupes de politiques d'accès, à la page 202. **Remarque** Vous devez définir les actions « Block, Monitor ou Warn » dans la section de filtrage des catégories YouTube de la page **Access Policies: URL Filtering** (Politiques d'accès : filtrage des URL).

Activation de la fonctionnalité de catégorisation de YouTube

Avant de commencer

- Activez le proxy HTTPS [**Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS)].
- Activez Acceptable Use Controls [**Security Services** > **Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable)].
- Configurez les catégories d'URL personnalisées et externes [**Web Security Manager** > **Custom and External URL Categories** (Web Security Manager > Catégories d'URL personnalisées et externes)] avec www.youtube.com et m.youtube.com.

- Configurez la politique de déchiffrement à l'aide de la catégorie d'URL personnalisées et externes pour YouTube, avec l'action « decrypt ».
- Générez la clé API Google à l'aide des services API Google pour YouTube Pour générer une clé API Google :
  1. Connectez-vous à https://console.developers.google.com/ à l'aide des informations d'authentification du compte Google. (Nous vous recommandons de ne pas utiliser votre compte Google personnel.)
  2. Créez un projet.
  3. Dans la zone **Enable APIs and Services** (Activer les API et les services), activez **YouTube Data API v3.**
  4. Générez une clé API à l'aide de l'assistant ou de l'option **Credentials** (Informations d'identification) sous **APIs & Services** (API et services).

Remarque Si vous générez la clé API à l'aide de l'assistant, sous **YouTube Data API v3** :

1. Dans la liste déroulante **Where will you be calling the API from?** (D'où appellerez-vous l'API?, choisissez **Other non-UI (e.g. cron job, daemon)** (Autre non-IU (par exemple, cron job, démon)).
2. Dans la section **What data will you be accessing** (À quelles données accéderez-vous), choisissez **Public data** (Données publiques).
3. Cliquez sur **What credentials do I need?** (De quelles informations d'identification ai-je besoin?), puis cliquez sur **Done** (Terminé).

Étape 1 Choisissez **Security Services** > **Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cochez la case Enable (Activer) à côté de la catégorisation YouTube.

Étape 4 Saisissez la clé API générée à l'aide des services API de Google.

Vous devez générer la clé API à l'aide des services d'API de Google avant d'activer la fonctionnalité de catégorisation de YouTube.

Étape 5 Saisissez le délai d'expiration de la demande pour définir le délai d'expiration entre l'appliance et le serveur d'API YouTube.

Étape 6 Choisissez la table de routage par laquelle passe le trafic de la catégorie YouTube :

- Data : Pour les interfaces P1 et P2
- Management : Pour l'interface M1

Remarque La table de routage par défaut est Data. Les deux options ci-dessus ne sont disponibles que si vous avez configuré deux tables de routage distinctes pour les services de données et de gestion (Network > Interfaces) (Réseau > Interfaces).

Étape 7 Envoyez et validez vos modifications.

Création et modification de catégories d'URL personnalisées

Vous pouvez créer des catégories URL de flux en direct personnalisées et externes qui décrivent des noms d'hôte et des adresses IP spécifiques. En outre, vous pouvez modifier et supprimer des catégories d'URL existantes. Lorsque vous incluez ces catégories d'URL personnalisées dans le même groupe d'accès, de déchiffrement ou de politique de sécurité des données Cisco et que vous affectez différentes actions à chaque catégorie, l'action de la catégorie d'URL personnalisée plus élevée prévaut.

Note Le nombre de fichiers de flux en direct externes qui peuvent être utilisés dans ces définitions de catégories d'URL est limité à 30 et chaque fichier ne doit pas contenir plus de 5 000 entrées. L'augmentation du nombre d'entrées de flux externe ou la présence d'un grand nombre d'entrées d'expressions régulières entraîne une dégradation des performances.

Secure Web Appliance utilise les quatre premiers caractères des noms de catégories d'URL personnalisées précédés de « c_ » dans les journaux d'accès. Envisagez le nom de la catégorie d'URL personnalisé si vous utilisez Sawmill pour analyser les journaux d'accès. Si les quatre premiers caractères de la catégorie d'URL personnalisée comprennent un espace, Sawmill ne peut pas analyser correctement l'entrée du journal des accès. Au lieu de cela, utilisez uniquement des caractères pris en charge dans les quatre premiers caractères. Si vous souhaitez inclure le nom complet d'une catégorie d'URL personnalisée dans les journaux d'accès, ajoutez le spécificateur de format %XF aux journaux d'accès.

Note Si le DNS résout plusieurs adresses IP en un site Web et si l'une de ces adresses IP figure dans une liste bloquée personnalisée, Secure Web Appliance bloque le site Web pour toutes les adresses IP, même si elles ne figurent pas dans la liste bloquée personnalisée.

Before you begin

Accédez à **Security Services** > **Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable) pour activer Acceptable Use Controls (Contrôles d'utilisation acceptable).

Étape 1 Choisissez **Web Security Manager > Custom and External URL Categories** (Web Security Manager > Catégories d'URL personnalisées et externes).

Étape 2 Pour créer une catégorie d'URL personnalisée, cliquez sur **Add Category** (Ajouter une catégorie). Pour modifier une catégorie d'URL personnalisée existante, cliquez sur le nom de la catégorie d'URL.

Étape 3 Indiquez les renseignements suivants.

Paramètres	Description
Category Name (Nom de la catégorie)	Entrez un identifiant pour cette catégorie d'URL. Ce nom s'affiche lorsque vous configurez le filtrage d'URL pour les groupes de politiques.

Paramètres	Description
List Order (Ordre de la liste)	Précisez l'ordre de cette catégorie dans la liste des catégories d'URL personnalisées. Entrez « 1 » pour la première catégorie d'URL de la liste. Le moteur de filtrage d'URL évalue une demande d'un client par rapport aux catégories d'URL personnalisées dans l'ordre spécifié.
Category Type (Type de catégorie)	Choisissez **Local Custom Category** (Catégorie personnalisée locale) ou **External Live Feed Category** (Catégorie de flux externe en direct).
Routing Table (Tableau de routage)	Choisissez **Management** (Gestion) ou **Data** (Données). Ce choix est disponible uniquement si le « routage fractionné » est activé; c'est-à-dire qu'elle n'est pas disponible avec les catégories personnalisées locales. Consultez Activation ou modification des interfaces réseau, on page 27 pour obtenir des renseignements sur l'activation du routage fractionné.

Sites / Feed File Location (Emplacement du fichier de sites/flux)	Si vous choisissez **Local Custom Category** (Catégorie de flux en direct externe) dans **Category Type** (Type de catégorie), indiquez les **Sites** personnalisés :
	• Entrez une ou plusieurs adresses de site pour cette catégorie personnalisée. Vous pouvez entrer plusieurs adresses séparées par des sauts de ligne ou des virgules. Ces adresses peuvent se présenter dans l'un des formats suivants :
	  • Adresse IPv4, p. ex. 10.1.1.0
	  • Adresse IPv6, p. ex. 2001:0db8::
	  • Adresse IPv4 CIDR, p. ex. 10.1.1.0/24
	  • Adresse IPv6 CIDR, p. ex. 2001:0db8::/32
	  • Nom de domaine, p. ex. exemple.com
	  • Nom d'hôte, p. ex. crm.exemple.com
	  • Nom d'hôte partiel, p. ex. exemple.com; cela correspondra également à www.exemple.com
	  • Des expressions régulières peuvent être saisies dans la section **Advanced** (Avancé), comme décrit ci-dessous.
	Note Il est possible d'utiliser la même adresse dans plusieurs catégories d'URL personnalisées, mais l'ordre dans lequel les catégories sont répertoriées est pertinent. Si vous incluez ces catégories dans la même politique et définissez différentes actions pour chacune, l'action définie pour la catégorie répertoriée en haut du tableau des catégories d'URL personnalisées sera celle appliquée.
	• (Facultatif) Cliquez sur **Sort URLs** (Trier les URL) pour trier toutes les adresses dans le champ Sites.
	Note Une fois que vous avez trié les adresses, vous ne pouvez pas récupérer leur ordre initial.

Paramètres	Description
Excluded Sites (Sites exclus)	Si vous choisissez **External Live Feed Category** (Catégorie de flux en direct externe) dans **Category Type** (Type de catégorie), indiquez les sites que vous souhaitez exclure du fichier de flux existant. Vous pouvez entrer plusieurs adresses séparées par des sauts de ligne ou des virgules. Ces adresses peuvent se présenter dans l'un des formats suivants : • Adresses IPv6 comme 2001:0db8::/32 • Adresses IPv4 comme 10.1.1.0. • Adresses CIDR IPv6 comme 2001:0db8::/32 • Adress CIDR IPv4 comme 10.1.1.0/24 • Nom de domaine, p. ex. exemple.com • Nom d'hôte, p. ex. crm.exemple.com • Nom d'hôte partiel, comme .exemple.com; correspondra également à www.exemple.com

Paramètres	Description
Feed Location (Emplacement du flux) (suite)	

Paramètres	Description
	Si vous choisissez **External Live Feed Category** (Catégorie de flux en direct externe) dans **Category Type** (Type de catégorie), renseignez le champ **Feed File Location** (Emplacement du fichier de flux); en d'autres termes, recherchez et téléchargez le fichier contenant les adresses pour cette catégorie personnalisée : **a.** Sélectionnez le **format de flux Cisco**, le **format de flux Office 365** ou **Office 365 Web Service**, et indiquez les informations appropriées sur les fichiers de flux. • **Format du flux Cisco** : • Choisissez le protocole de transport à utiliser (HTTPS ou HTTP), puis saisissez l'URL du fichier de flux en direct. Ce fichier doit être un fichier au format .csv (valeurs séparées par des virgules). Consultez Formats des fichiers de flux externes, on page 217 pour plus d'informations sur ce fichier. • Vous pouvez également fournir les informations d'**authentification** dans la section **Advanced** (Avancé). Indiquez un nom d'utilisateur et une phrase secrète à utiliser pour la connexion au serveur de flux précisé. • **Format de flux Office 365** : • Entrez l'**emplacement du flux Office 365** (URL) du fichier de flux en direct. Ce fichier doit être au format XML; consultez Formats des fichiers de flux externes, on page 217 pour en savoir plus sur ce fichier. • **Office 365 Web Service** Saisissez l'URL du service Web. Elle ne doit pas contenir de ClientRequestId et elle doit se présenter au format JSON. L'appliance génère automatiquement le ClientRequestId. **b.** Pour les formats de flux Cisco et Office 365, cliquez sur **Get File** (Obtenir le fichier) pour tester la connexion au serveur de flux, puis analysez et téléchargez le fichier de flux à partir du serveur. La progression est affichée dans la zone de texte sous le bouton **Get File** (Obtenir le fichier). Si une erreur se produit, le problème est indiqué et doit être rectifié avant de réessayer. Reportez-vous à Problèmes de téléchargement d'un fichier de flux en direct externe, on page 648 pour en savoir plus sur les erreurs possibles. Pour Office 365 Web Service, cliquez sur **Start Test** (Démarrer le test) pour lancer le service et télécharger les URL et les adresses IP. **Note** Vous ne pouvez pas utiliser plus de 30 fichiers de flux en direct externes dans ces définitions de catégories d'URL, et chaque fichier ne doit pas contenir plus de 5 000 entrées. L'augmentation du nombre d'entrées de flux externe entraîne une dégradation des performances. **Tip** Après avoir enregistré vos modifications pour cette catégorie de flux en direct, vous pouvez cliquer sur **View** (Afficher) dans la colonne **Feed Content** (Contenu du flux) pour cette entrée dans la page Custom and External URL Categories (Catégories d'URL personnalisées et externes) (**Web Security Manager** > **Custom**

Paramètres	Description
	and External URL Categories (Web Security Manager > Catégories d'URL personnalisées et externes)) pour ouvrir une fenêtre qui affiche le adresses contenues dans le fichier de flux Cisco Flow ou Office 365 que vous avez téléchargé ici.
Advanced (Niveau avancé)	Si vous choisissez **Local Custom Category** (Catégorie personnalisée locale) comme type de catégorie, vous pouvez saisir des expressions régulières dans cette section pour spécifier des ensembles d'adresses supplémentaires. Vous pouvez utiliser des expressions régulières pour spécifier plusieurs adresses qui correspondent aux schémas que vous saisissez. **Note** • Le moteur de filtrage d'URL compare d'abord les URL avec les adresses saisies dans le champ Sites. Si l'URL d'une transaction correspond à une entrée dans le champ Sites, elle n'est comparée à aucune expression saisie ici. • Utilisez « %20 » au lieu d'un espace lors de l'ajout des chemins d'URL en tant qu'expressions régulières. Les chemins d'accès URL ne doivent pas contenir d'espaces lorsqu'ils sont utilisés comme expressions régulières. Consultez Expressions régulières, on page 224 pour plus d'informations sur l'utilisation des expressions régulières.
Advanced (Exclude Regular Expresions) [Avancé (sauf les expressions régulières)]	Si vous choisissez **External Live Feed Category**(Catégorie de flux en direct externe) comme **Type de catégorie**, saisissez les expressions régulières que vous souhaitez exclure du fichier de flux existant. Les entrées doivent correspondre exactement aux expressions régulières existantes dans le fichier de flux.
Auto Update the Feed (Mettre à jour automatiquement le flux)	Choisissez une option de mise à jour de flux : • **Ne pas mettre à jour automatiquement** • **Chaque *n* HH:MM**; par exemple, entrez 00:05 pour cinq minutes. Cependant, notez qu'une mise à jour fréquente peut affecter les performances de Secure Web Appliance. **Note** À chaque rechargement et à chaque nouvelle publication, l'appliance télécharge le fichier de flux disponible et met à jour l'heure de téléchargement, même si le fichier de flux disponible est le même que celui actuellement téléchargé.

Étape 4 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Expressions régulières, on page 224.
- Personnalisation des journaux d'accès, on page 523.
- Problèmes liés aux catégories d'URL personnalisées et externes, on page 648

Formats d'adresse et formats de fichier de flux pour les catégories d'URL personnalisées et externes

Lors de la création et de la modification de catégories URL personnalisées et externes, vous devez indiquer une ou plusieurs adresses réseau, que ce soit pour un fichier de flux de **catégorie personnalisée locale** ou de **catégorie de flux en direct externe**. Dans chaque cas, vous pouvez entrer plusieurs adresses séparées par des sauts de ligne ou des virgules. Ces adresses peuvent se présenter dans l'un des formats suivants :

- Adresse IPv4, p. ex. 10.1.1.0
- Adresse IPv6, p. ex. 2001:0db8::
- Adresse IPv4 CIDR, p. ex. 10.1.1.0/24
- Adresse IPv6 CIDR, p. ex. 2001:0db8::/32
- Nom de domaine, p. ex. exemple.com
- Nom d'hôte, p. ex. crm.exemple.com
- Nom d'hôte partiel, p. ex. exemple.com; cela correspondra également à www.exemple.com
- Des expressions régulières pour spécifier plusieurs adresses qui correspondent aux modèles fournis (voir Expressions régulières, à la page 224 pour plus d'informations sur l'utilisation des expressions régulières)

Remarque Il est possible d'utiliser la même adresse dans plusieurs catégories d'URL personnalisées, mais l'ordre dans lequel les catégories sont répertoriées est pertinent. Si vous incluez ces catégories dans la même politique et définissez différentes actions pour chacune, l'action définie pour la catégorie répertoriée en haut du tableau des catégories d'URL personnalisées sera celle appliquée.

Formats des fichiers de flux externes

Si vous sélectionnez **External Live Feed Category** (Catégorie de flux en direct) dans **Category Type** (Type de catégorie) lors de la création et de la modification des catégories d'URL personnalisées et externes, vous devez sélectionner le format de flux (**Cisco Feed Format** ou **Office 365 Feed Format**), puis fournir une URL vers le serveur de fichiers de flux approprié.

Le format attendu pour chaque fichier de flux est le suivant :

- **Format de flux Cisco** : il doit s'agir d'un fichier de valeurs séparées par des virgules (.csv); c'est-à-dire un fichier texte avec une extension .csv. Chaque entrée du fichier .csv doit se trouver sur une ligne distincte, comme suit address/comma/addresstype (par exemple : `www.cisco.com,site` ou `ad2.*\.com`,regex). Les types d'adresses valides sont `site` et `regex`. Voici un extrait d'un fichier de flux de Cisco au format .csv :

```
www.cisco.com,site

\.xyz,regex

ad2.*\.com,regex

www.trafficholder.com,site
```

```
2000:1:1:11:1:1::200,site
```

Remarque N'incluez pas `http://` ou `https://` dans une entrée `site` dans le fichier, sinon une erreur se produira. En d'autres termes, `www.exemple.com` est analysé correctement, tandis que `http://www.exemple.com` produit une erreur.

- **Format de flux Office 365** – Il s'agit d'un fichier XML situé sur un serveur Microsoft Office 365 ou sur un serveur local sur lequel vous avez enregistré le fichier. Il est fourni par le service Office 365 et ne peut pas être modifié. Les adresses réseau dans le fichier sont délimitées par des balises XML, en respectant la structure suivante : `produits > produit – liste d'adresses > adresse`. Dans l'implémentation actuelle, un type de `liste d'adresses` peut être IPv6, IPv4 ou URL (qui peut inclure des domaines et des schémas d'expression régulière). Voici un extrait d'un fichier de flux Office 365 :

```
<products updated="4/15/2016">
   <product name="o365">
      <addresslist type="IPv6">
         <address>2603:1040:401::d:80</address>
         <address>2603:1040:401::a</address>
         <address>2603:1040:401::9</address>
      </addresslist>
      <addresslist type="IPv4">
         <address>13.71.145.72</address>
         <address>13.71.148.74</address>
         <address>13.71.145.114</address>
      </addresslist>
      <addresslist type="URL">
         <address>*.aadrm.com</address>
         <address>*.azurerms.com</address>
         <address>*.cloudapp.net2</address>
      </addresslist>
   </product>
   <product name="LYO">
      <addresslist type="URL">
         <address>*.broadcast.skype.com</address>
         <address>*.Lync.com</address>
      </addresslist>
```

```
    </product>
  </products>
```

Filtrage du contenu pour adultes

Vous pouvez configurer Secure Web Appliance pour filtrer le contenu pour adultes de certaines recherches sur le Web et certains sites Web. Pour appliquer une recherche sécurisée et une évaluation du contenu de site, le moteur AVC tire parti de la fonctionnalité de mode sans échec mise en œuvre sur un site Web particulier en réécrivant les URL et/ou des témoins Web pour forcer le mode sans échec.

Les fonctionnalités suivantes filtrent le contenu pour adultes :

Option	Description
Enforce safe searches (Appliquer des recherches sécurisées)	Vous pouvez configurer Secure Web Appliance pour que les demandes de recherche sortantes apparaissent pour les moteurs de recherche comme des demandes de recherche sécurisées. Cela peut empêcher les utilisateurs de contourner les politiques d'utilisation acceptable des moteurs de recherche.
Enforce site content ratings (Appliquer l'évaluation du contenu du site)	Certains sites de partage de contenu permettent aux utilisateurs de restreindre leur propre accès au contenu pour adultes de ces sites soit en appliquant leur propre fonction de recherche sécurisée, soit en bloquant l'accès au contenu pour adultes, ou les deux. Cette fonctionnalité de classification est communément appelée évaluation du contenu.

Note Toute politique d'accès pour laquelle la fonction de recherche sécurisée ou d'évaluation du contenu du site est activée est considérée comme une politique d'accès pour une navigation en toute sécurité.

Application des méthodes de recherche sécurisée et d'évaluation du contenu du site

Note Lorsque vous activez la recherche sécurisée ou l'évaluation du contenu du site, le moteur AVC est chargé d'identifier les applications pour une navigation en toute sécurité. Parmi les critères, le moteur AVC analysera le corps de la réponse pour détecter une application de recherche. Par conséquent, l'appliance ne transférera pas les en-têtes de plage.

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien sous la colonne URL Filtering (Filtrage d'URL) pour un groupe de politiques d'accès ou le groupe de politiques global.

Étape 3 Lorsque vous modifiez une politique d'accès définie par l'utilisateur, choisissez Define Content Filtering Personnalisé Settings dans la section Content Filtering.

Étape 4 Cochez la case **Enable Safe Search** (Activer la recherche sécurisée) pour activer la fonction de recherche sécurisée.

Étape 5 Choisissez si vous souhaitez bloquer les utilisateurs des moteurs de recherche qui ne sont pas actuellement pris en charge par la fonctionnalité de recherche sécurisée Secure Web Appliance.

Étape 6 Cochez la case **Enable Site Content Evaluation (** Activer l'évaluation du contenu du site) pour activer la fonction d'évaluation du contenu du site.

Étape 7 Choisissez si vous souhaitez bloquer tout le contenu pour adultes des sites Web de classification de contenu pris en charge ou pour afficher la page d'avertissement de filtrage d'URL de l'utilisateur final.

Note Lorsque l'URL de l'un des moteurs de recherche ou des sites Web de classification de contenu pris en charge est incluse dans une catégorie d'URL personnalisée avec l'action Allow (Autoriser), aucun résultat de recherche n'est bloqué et tout le contenu est visible.

Étape 8 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Aviser les utilisateurs et leur permettre de continuer, on page 222.

Journalisation de l'accès au contenu pour adultes

Par défaut, les journaux d'accès comprennent un verdict d'analyse de navigation sécurisée entre les crochets obliques de chaque entrée. Le verdict d'analyse de navigation sécurisée indique si la recherche sécurisée ou la fonction d'évaluation du contenu du site a été appliquée à la transaction. Vous pouvez également ajouter la variable de verdict de l'analyse pour la navigation de sécurité aux journaux d'accès ou aux journaux d'accès W3C :

- Journaux d'accès : %XS
- Journaux d'accès W3C : x-request-rewrite

Valeur	Description
ensrch	La demande initiale du client n'était pas sécurisée et la fonctionnalité de recherche sécurisée a été appliquée.
encrt	La demande initiale du client n'était pas sécurisée et la fonction d'évaluation du contenu du site a été appliquée.
unsupp	La demande initiale du client allait à un moteur de recherche non pris en charge.
err	La demande initiale du client était dangereuse, mais ni la recherche sécurisée ni la fonction d'évaluation du contenu du site n'ont pu être appliquées en raison d'une erreur.

Valeur	Description
-	Ni la recherche sécurisée ni la fonction d'évaluation du contenu du site n'ont été appliquées à la demande du client, car les fonctionnalités ont été contournées (par exemple, la transaction a été autorisée dans une catégorie d'URL personnalisée) ou la demande a été faite à partir d'une application non prise en charge.

Les demandes bloquées en raison des fonctionnalités de recherche sécurisée ou de classification du contenu du site, utilisez l'une des balises de décision ACL suivantes dans les journaux d'accès :

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

Thèmes connexes

- Balises de décision ACL, on page 505.

Redirection du trafic dans les politiques d'accès

Vous pouvez configurer Secure Web Appliance pour rediriger le trafic destiné à l'origine à une URL dans une catégorie d'URL personnalisée vers un emplacement que vous spécifiez. Cela vous permet de rediriger le trafic vers l'appliance plutôt que vers le serveur de destination. Vous pouvez rediriger le trafic pour un groupe de politiques d'accès personnalisé ou pour le groupe de politiques global.

Before you begin

Pour rediriger le trafic, vous devez définir au moins une catégorie d'URL personnalisée.

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien sous la colonne URL Filtering (Filtrage d'URL) pour un groupe de politiques d'accès ou le groupe de politiques global.

Étape 3 Dans la section de filtrage des catégories d'URL personnalisées, cliquez sur **Select Custom Categories** (Sélectionner des catégories personnalisées).

Étape 4 Dans la boîte de dialogue **Select Custom Categories for this Policy** (Sélectionner des catégories personnalisées pour cette politique), choisissez **Include in policy** (Inclure dans la politique) pour la catégorie d'URL personnalisée que vous souhaitez rediriger.

Étape 5 Cliquez sur **Apply** (Appliquer).

Étape 6 Cliquez dans la colonne Redirect (Rediriger) pour la catégorie personnalisée que vous souhaitez rediriger.

Étape 7 Entrez l'URL vers laquelle vous souhaitez rediriger le trafic dans le champ **Redirect To** (Rediriger vers) de la catégorie personnalisée.

Étape 8 Envoyez et validez les modifications.

Note Méfiez-vous des boucles infinies lorsque vous configurez l'appliance pour rediriger le trafic.

What to do next

Thèmes connexes

- Création et modification de catégories d'URL personnalisées, on page 211

Journalisation et création de rapports

Lorsque vous redirigez le trafic, l'entrée du journal des accès au site Web initialement demandé comporte une balise ACL qui commence par REDIRECT_CUSTOMCAT. Plus tard dans le journal des accès (généralement sur la ligne suivante), l'entrée du site Web vers lequel l'utilisateur a été redirigé apparaît.

Les rapports affichés sous l'onglet Rapports affichent les transactions redirigées comme « Autorisées ».

Aviser les utilisateurs et leur permettre de continuer

Vous pouvez avertir les utilisateurs qu'un site ne respecte pas les politiques d'utilisation acceptable d'une organisation. Les utilisateurs sont suivis dans le journal des accès par nom d'utilisateur si l'authentification a rendu un nom d'utilisateur disponible, et par adresse IP si aucun nom d'utilisateur n'est disponible.

Vous pouvez avertir et autoriser les utilisateurs à continuer en utilisant l'une des méthodes suivantes :

- Choisissez l'action Warn (Avertir) pour une catégorie d'URL dans un groupe de politiques d'accès ou
- Activez la fonction d'évaluation du contenu du site et avertissez les utilisateurs qui accèdent au contenu pour adultes au lieu de les bloquer.

Configuration des paramètres de la page d'avertissement de filtrage de l'utilisateur final

Note

- La fonction Warn and Continue (Avertir et continuer) ne fonctionne que pour les transactions HTTP et HTTPS déchiffré. Elle ne fonctionne pas avec les transactions FTP natives.
- Lorsque le moteur de filtrage d'URL avertit les utilisateurs au sujet d'une demande particulière, il affiche une page d'avertissement que le proxy Web envoie à l'utilisateur final. Cependant, tous les sites Web n'affichent pas la page d'avertissement à l'utilisateur final. Lorsque cela se produit, les utilisateurs sont bloqués au niveau de l'URL à laquelle est affectée l'option Warn (Avertir) sans avoir la possibilité de continuer à accéder au site de quelque façon que ce soit.

Étape 1 Choisissez **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Configurez les paramètres suivants sur la page **End-User Filtering Warning** (Avertissement concernant le filtrage à l'utilisateur final :

Option	Méthode
Time Between Warning (Intervalle entre les avertissements)	L'intervalle entre les avertissements détermine la fréquence à laquelle le proxy Web affiche la page d'avertissement relative au filtrage des URL à l'attention de l'utilisateur final pour chaque catégorie d'URL par utilisateur. Ce paramètre s'applique aux utilisateurs suivis par nom d'utilisateur et aux utilisateurs suivis par adresse IP. Indiquez une valeur comprise entre 30 et 2678400 secondes (un mois). La valeur par défaut est 1 heure (3 600 secondes).
Custom Message (Message personnalisé)	Le message personnalisé est du texte que vous saisissez en vue de l'afficher sur chaque page d'avertissement relative au filtrage d'URL à l'attention de l'utilisateur final. Incluez des balises HTML simples pour mettre en forme le texte.

Étape 4 Cliquez sur Submit (soumettre).

What to do next

Thèmes connexes

- Filtrage du contenu pour adultes, on page 219
- Messages personnalisés sur les pages de notification, on page 382
- Configuration de la page d'avertissement du filtrage des URL de l'utilisateur final, on page 381

Création de filtres d'URL basés sur le temps

Vous pouvez configurer la façon dont Secure Web Appliance gère les demandes d'URL dans des catégories particulières différemment selon l'heure et le jour.

Before you begin

Accédez à la page **Web Security Manager > Defined Time Range** (Web Security Manager > Plage de temps définie) pour définir au moins une plage de temps.

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans le tableau des politiques, sous la colonne URL Filtering (Filtrage d'URL), pour le groupe de politiques que vous souhaitez modifier.

Étape 3 Sélectionnez **Time-Based** (Basé sur le temps) pour la catégorie d'URL personnalisée ou prédéfinie que vous souhaitez configurer en fonction de la plage de temps.

Étape 4 Dans le champ **In Time Range** (Dans la plage de temps), choisissez la plage de temps définie à utiliser pour la catégorie d'URL.

Étape 5 Dans le champ **Action**, choisissez l'action à appliquer aux transactions de cette catégorie d'URL pendant la plage de temps définie.

Étape 6 Dans le champ **Otherwise** (Sinon), choisissez l'action à appliquer aux transactions de cette catégorie d'URL en *dehors* de la plage de temps définie.

Étape 7 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Plages de temps et quotas, on page 269

Affichage de l'activité de filtrage d'URL

La page **Reporting > URL Categories** (Rapports > Catégories d'URL) fournit un affichage collectif des statistiques d'URL qui comprennent des informations sur les principales catégories d'URL mises en correspondance et les principales catégories d'URL bloquées. Cette page affiche des données spécifiques à la catégorie pour les économies de bande passante et les transactions Web.

Thèmes connexes

- Générer des rapports pour superviser l'activité de l'utilisateur final, on page 399

Interprétation des données non filtrées et non classées

Lors de l'affichage des statistiques d'URL sur la page Reporting > URL Categories (Rapports > Catégories d'URL), il est important de comprendre comment interpréter les données suivantes :

Type de données	Description
URL Filtering Bypassed (Filtrage des URL contourné)	Représente le blocage de politiques, de ports et d'agents utilisateur admin qui se produit avant le filtrage d'URL.
Uncategorized URL (URL non classées)	Représente toutes les transactions pour lesquelles le moteur de filtrage d'URL est interrogé, mais aucune catégorie ne correspond.

Journalisation des catégories d'URL dans les journaux d'accès

Le fichier journal des accès enregistre la catégorie d'URL pour chaque transaction dans la section des renseignements sur le verdict d'analyse de chaque entrée.

Thèmes connexes

- Superviser l'activité du système au moyen de journaux, on page 483.
- Descriptions des catégories d'URL, on page 228.

Expressions régulières

Secure Web Appliance utilise une syntaxe d'expression régulière qui diffère légèrement de la syntaxe d'expression régulière utilisée par les autres implémentations du moteur de mise en correspondance avec le modèle Velocity. En outre, l'appliance ne prend pas en charge l'utilisation d'une barre oblique inverse pour

éviter une barre oblique. Si vous devez utiliser une barre oblique dans une expression régulière, saisissez simplement la barre oblique sans barre oblique inverse.

Note Techniquement, AsyncOS pour le Web utilise l'analyseur d'expression régulière Flex.

Vous pouvez utiliser des expressions régulières aux emplacements suivants :

- **Catégories d'URL personnalisées pour les politiques d'accès.** Lorsque vous créez une catégorie d'URL personnalisée à utiliser avec des groupes de politiques d'accès, vous pouvez utiliser des expressions régulières pour spécifier plusieurs serveurs Web correspondant au schéma que vous saisissez. Le nombre maximal de caractères qui peuvent être utilisés dans les expressions régulières a été fixé à 2048 pour restreindre toute vulnérabilité de sécurité Web.
- **Agents utilisateurs personnalisés à bloquer** Lorsque vous modifiez les applications à bloquer pour un groupe de politiques d'accès, vous pouvez utiliser des expressions régulières pour saisir des agents utilisateurs spécifiques à bloquer.

Note Les expressions régulières qui effectuent des correspondances de caractères étendues consomment des ressources et peuvent affecter les performances du système. Pour cette raison, les expressions régulières doivent être appliquées avec prudence.

Thèmes connexes

- Création et modification de catégories d'URL personnalisées, on page 211

Création d'expressions régulières

Les expressions régulières sont des règles qui utilisent généralement le mot « matches » (correspondances) dans les expressions. Elles peuvent être appliquées pour la correspondance à des destinations d'URL ou à des serveurs Web précis. Par exemple, l'expression régulière suivante correspond à tout modèle contenant « `blocksite.com` » :

```
\.blocksite\.com
```

Considérez l'exemple d'expression régulière suivant :

```
server[0-9]\.example\.com
```

Dans cet exemple, `server[0-9]` correspond à `server0`, `server1`, `server2`, ..., `server9` dans le domaine `exemple.com`.

Dans l'exemple suivant, l'expression régulière correspond aux fichiers se terminant par `.exe`, `.zip` et `.bin` dans le répertoire des téléchargements.

```
/downloads/.*\.(exe|zip|bin)
```

Note Vous devez mettre les expressions régulières qui contiennent des espaces ou des caractères non alphanumériques entre guillemets ASCII.

Directives pour éviter les échecs de validation

Important : Les expressions régulières qui renvoient plus de 63 caractères échoueront et produiront une erreur d'entrée non valide. Assurez-vous de former des expressions régulières qui ne peuvent pas renvoyer plus de 63 caractères.

Suivez ces directives pour minimiser les échecs de validation :

- Utilisez des expressions littérales plutôt que des caractères génériques et des expressions entre crochets chaque fois que cela est possible. Une expression littérale ne se compose essentiellement que de texte tel que « `C'est aussi facile que ABC123` ». La probabilité d'échec est moins grande que d'utiliser « `C'est aussi facile que [AC]{3}[1-3]{3}` ». Cette dernière expression entraîne la création d'entrées d'automates finis (NFA) non déterministes, ce qui peut considérablement augmenter le temps de traitement.
- Évitez autant que possible l'utilisation d'un point sans échappement. Le point est un caractère d'expression régulière spéciale qui signifie qu'il correspond à n'importe quel caractère, à l'exception d'un retour à la ligne. Si vous souhaitez mettre en correspondance un point réel, par exemple, comme dans « `url.com` », alors ajoutez un échappement au point en utilisant le caractère \, comme dans « `url\.com` ». Les points avec échappement sont traités comme des entrées littérales et ne causent donc pas de problèmes.
- Tout point sans échappement dans un schéma qui renverra plus de 63 caractères après le point sera désactivé par le moteur de recherche de schéma; une alerte à cet effet vous sera envoyée, et vous continuerez à recevoir une alerte après chaque mise à jour jusqu'à ce que vous corrigiez ou remplaciez ce schéma.

  De même, utilisez plus de correspondances spécifiques plutôt que des points sans échappement chaque fois que cela est possible. Par exemple, si vous souhaitez mettre en correspondance une URL suivie d'un seul chiffre, utilisez « `url[0-9]` » plutôt que « `url.`».
- Les points sans échappement dans une expression régulière plus longue peuvent être particulièrement problématiques et doivent être évités. Par exemple, « `Il y a quatre-vingt-sept ans, nos pères ont donné naissance sur ce continent à une nouvelle nation, conçue dans la Liberté et adhérant à l'idée que tous les êtres humains sont .gaux` » peut entraîner un échec. Le remplacement du point dans « `.gaux` » par l'expression littérale « `égaux` » devrait résoudre le problème.

  En outre, un point sans échappement dans un schéma qui renverra plus de 63 caractères après le point sera désactivé par le moteur de mise en correspondance de schéma. Corrigez ou remplacez le schéma.
- Vous ne pouvez pas utiliser « `.*` » pour commencer ou terminer une expression régulière. Vous ne pouvez pas non plus utiliser « `./` » dans une expression régulière destinée à correspondre à une URL, et vous ne pouvez pas non plus terminer une telle expression par un point.
- Les combinaisons de caractères génériques et d'expressions entre crochets peuvent provoquer des problèmes. Éliminez le plus de combinaisons possible. Par exemple, « `id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$` » peut provoquer un échec, tandis que « `Gecko/20100101 Firefox/9\.0\.1\$` » n'entraînera pas d'erreur. Cette dernière expression ne comprend aucun caractère générique ni expression entre crochets, et les deux expressions n'utilisent que des points avec échappement.

Lorsque les caractères génériques et les expressions entre crochets ne peuvent pas être éliminés, essayez de réduire la taille et la complexité de l'expression. Par exemple, « `[0-9a-z]{64}` » peut provoquer un échec. La remplacer par une expression plus petite ou moins complexe, telle que « `[0-9]{64}` » ou « `[0-9a-z]{40}` » peut résoudre le problème.

Si un échec se produit, essayez de le résoudre en appliquant les règles précédentes aux expressions génériques (comme *, + et .) et entre crochets.

Note Vous pouvez utiliser l'option de l'interface de ligne de commande `advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex?` (Voulez-vous activer la conversion d'URL minuscules pour l'expression régulière de vitesse?) pour activer ou désactiver la conversion de l'expression régulière par défaut en minuscules pour la correspondance insensible à la casse. À utiliser si vous rencontrez des problèmes de respect de la casse. Pour plus d'informations sur cette option, consultez Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671.

Tableau de caractères d'expressions régulières

Méta-caractère	Description
.	Correspond à n'importe quel caractère, à l'exception du caractère de retour à la ligne (0x0A). Par exemple, l'expression régulière rt correspond aux chaînes rat, rut, r t, mais pas root. Méfiez-vous des points sans échappement dans les longs schémas, en particulier au milieu des schémas longs. Consultez Directives pour éviter les échecs de validation, on page 226 pour obtenir de plus amples renseignements.
*	Correspond à zéro ou plusieurs occurrences du caractère précédent immédiatement. Par exemple, l'expression régulière .* signifie qu'elle correspond à n'importe quelle chaîne de caractères et [0-9]* à n'importe quelle chaîne de chiffres. Méfiez-vous de l'utilisation de ce méta-caractère, en particulier conjointement avec le point. Tout schéma contenant un point sans échappement qui renvoie plus de 63 caractères après le point sera désactivé. Consultez Directives pour éviter les échecs de validation, on page 226 pour obtenir de plus amples renseignements.
\	Le caractère d'échappement; cela signifie traiter le méta-caractère suivant comme un caractère ordinaire. Par exemple, \^ est utilisé pour mettre en correspondance le signe d'insertion (^) plutôt que le début d'une ligne. De même, l'expression \. est utilisé pour correspondre à un point plutôt qu'à un caractère unique.
^	Correspond au début d'une ligne. Par exemple, l'expression régulière ^When in correspond au début de la chaîne « When in the cours of humain Events » mais pas à la chaîne « What and When in the ».
$	Correspond à la fin d'une ligne ou d'une chaîne. Par exemple, b$\. correspond à toute ligne ou chaîne se terminant par « b ».

Méta-caractère	Description
+	Correspond à une ou plusieurs occurrences du caractère ou de l'expression régulière qui le précède immédiatement. Par exemple, l'expression régulière 9+ correspond à 9, 99 et 999.
?	Correspond à zéro ou une occurrence de l'élément de modèle précédent. Par exemple, couleur correspond à la fois à « couleur » et à « color », car le « u » est facultatif.
( )	Traitez l'expression entre les parenthèses gauche et droite comme un groupe, en réduisant la portée des autres méta-caractères. Par exemple, (abc)+ correspond à une ou plusieurs occurrences de la chaîne « abc »; tels que « abcabcabc » ou « abc123 », mais pas « abab » ni « ab123 ».
|	OU logique : correspond au modèle précédent ou au modèle suivant. Par exemple, (him|her) correspond à la ligne « cela lui appartient » et à la ligne « cela lui appartient », mais ne correspond pas à la ligne « cela lui appartient ».
[ ]	Correspond à l'un des caractères entre parenthèses. Par exemple, l'expression régulière r[aou]t correspond à « rat », « rot » et « rut », mais pas à « ret ». Les plages de caractères sont spécifiées par un caractère de début, un tiret et un caractère de fin. Par exemple, le modèle [0-9] signifie correspondre à n'importe quel chiffre. Plusieurs plages peuvent également être spécifiées. Le modèle [A-Za-z] signifie correspondre à n'importe quelle lettre majuscule ou minuscule. Pour mettre en correspondance n'importe quel caractère, à l'exception de ceux de la plage (c'est-à-dire la plage complémentaire), utilisez un signe d'insertion comme premier caractère après le crochet ouvrant. Par exemple, l'expression [^269A-Z] correspond à tous les caractères sauf 2, 6, 9 et les lettres majuscules.
{ }	Spécifie le nombre de fois où correspondre au modèle précédent. Par exemple : D{1,3} correspond à une à trois occurrences de la lettre D Correspond à un nombre spécifique {**n**} ou à un nombre minimal {**n**} d'instances du modèle précédent. Par exemple, l'expression A[0-9]{3} correspond à « A » suivi d'exactement trois chiffres. C'est-à-dire qu'il correspond à « A123 », mais pas à « A1234 ». L'expression [0-9]{4,} correspond à toute séquence de quatre chiffres ou plus.
"..."	Interpréter littéralement tous les caractères mis entre guillemets.

Descriptions des catégories d'URL

Cette section répertorie les catégories d'URL pour Cisco Web Usage Controls. Les tableaux comprennent également les noms abrégés des catégories d'URL qui peuvent s'afficher dans la section de filtrage de réputation Web et d'analyse de protection contre les programmes malveillants d'une entrée de fichier de journal des accès.

Note Dans les journaux d'accès, les abréviations de catégories d'URL pour Cisco Web Usage Controls comprennent le préfixe « IW_ » avant chaque abréviation, de sorte que la catégorie « art » devient « IW_art ».

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Adulte	adlt	1006	Destiné aux adultes, mais pas nécessairement à caractère pornographique. Peut inclure des boîtes pour adultes (boîtes de striptease, boîtes échangistes, services d'escorte, stripteaseuses); des renseignements généraux sur le sexe, non pornographiques; piercing d'organes génitaux; produits ou cartes de vœux pour adultes; informations sur des activités sexuelles en dehors du hors contexte de la santé ou des maladies.	www.adultentertainmentexpo.com www.sincerelynot.com
Publicités	pub	1027	Bannières et fenêtres contextuelles qui accompagnent souvent une page Web; d'autres sites Web publicitaires fournissant du contenu publicitaire. Les services et les ventes de publicité sont classés comme « entreprises et industrie ».	www.adforce.com www.doubleclick.com
Alcool	alc	1077	Alcool comme activité de plaisir; fabrication de bière et de vin, recettes de cocktails; vendeurs d'alcools, caves à vin, vignobles, brasseries, distributeurs d'alcool. L'alcoolisme est classé dans la catégorie « Santé et médecine ». Les bar et les restaurants sont classés dans la catégorie « Restauration et débit de boisson ».	www.samueladams.com www.whisky.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Animaux et animaux de compagnie	animaux de compagnie	1107	Informations sur les animaux de compagnie, bétail et animaux d'assistance, ainsi que les soins qui leur sont dispensés. Services vétérinaires, médicaments et santé animalière. Dressage d'animaux de compagnie et d'animaux, aquariums, zoos et spectacles animaliers. Comprend les refuges pour animaux, les sociétés humanitaires, les organismes de bienfaisance et les sanctuaires centrés sur les animaux, l'apiculture, la formation et l'élevage; dinosaures et animaux disparus.	www.petmd.com www.wheatenorg.uk
Arts	art	1002	Galeries et expositions; artistes et art; photographie; littérature et livres; arts du spectacle et théâtre; comédies musicales; ballet; musées; conception; architecture. Le cinéma et la télévision sont classés dans la catégorie « Divertissement ».	www.moma.org www.nga.gov
Astrologie	astr	1074	Astrologie; horoscope; voyance; numérologie; consultation de voyants; tarot.	www.astro.com www.astrology.com
Ventes aux enchères	ench	1088	Enchères en ligne et hors ligne, maisons de ventes aux enchères et petites annonces.	www.craigslist.com www.ebay.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Entreprise et industrie	entrep	1019	Marketing, commerce, sociétés, pratiques commerciales, main-d'œuvre, ressources humaines, transport, paie, sécurité et capital-risque; fournitures de bureau; équipements industriels (équipements de production), machines et systèmes mécaniques; matériel de chauffage, matériel de refroidissement; matériel de manutention; équipement d'emballage; fabrication : manutention de solides, fabrication de métaux, construction et bâtiment; transport de passagers; commerce; conception industrielle; construction, matériaux de construction; expédition et fret (services de fret, camionnage, transitaires, transporteurs de lots complets, courtiers de fret et de transport, services accélérés, correspondance de chargement et de fret, suivi et traçabilité, transport ferroviaire, transport maritime, services de transport routier, déménagement et entreposage).	www.freightcenter.com www.ge.com
Cannabis	cann	1109	Sites Web axés sur la consommation récréative et médicinale du cannabis. Les sites peuvent inclure du marketing, des discussions sur des questions juridiques et réglementaires, la culture et la production, le matériel, la recherche et l'investissement dans l'industrie du cannabis. Les dispensaires, les produits à base de cannabinoïdes (huile de CBD, THC, etc.) sont également inclus.	www.localproduct.co www.oregonbc.com
Clavardage et messagerie instantanée	clavarder	1040	Messagerie instantanée et salons de discussion sur le Web.	www.icq.com www.e-chat.co
Tricherie et plagiat	plag	1051	Promotion de la tricherie et vente de travaux écrits, tels que des dissertations, pour plagiat.	www.bestessays.com www.superiorpapers.com
Contenu maltraitant envers les enfants	cprn	1064	Contenu illégal d'exploitation sexuelle d'enfants dans le monde entier.	—

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Infonuagique et centres de données	serv	1118	Plateformes utilisées pour servir l'infrastructure infonuagique ou l'hébergement du centre de données afin de prendre en charge les applications, les services ou le traitement des données d'une organisation. En raison de la nature décentralisée de ces domaines et adresses IP, une catégorie plus spécifique ne peut pas être appliquée en fonction du contenu ou de la propriété.	www.azurewebsites.net www.s3.amazonaws.com
Sécurité informatique	csec	1065	Offre de produits et de services de sécurité pour les entreprises et les particuliers.	www.computersecurity.com www.symantec.com
Ordinateurs et Internet	comp	1003	Informations sur les ordinateurs et les logiciels, tels que le matériel, les logiciels, le support logiciel; informations pour les ingénieurs logiciels, programmation et réseaux; conception de sites Web; web et Internet en général; informatique; infographie et clipart. Les « gratuiciels et partagiciels » constituent une catégorie distincte.	www.xml.com www.w3.org
Congrès, conférences et salons professionnels	expo	1110	Séminaires, salons professionnels, conventions et conférences sur le thème d'un secteur, d'un marché ou d'un intérêt commun particulier. Peut inclure des informations sur l'achat de billets, l'inscription, les directives de proposition de résumé ou de présentation, les ateliers, les détails du parrainage, les informations sur les fournisseurs ou les exposants et tous autres supports de marketing ou de promotion. Cette catégorie inclut les événements académiques, professionnels ainsi que les événements de culture populaire, qui sont généralement tous des événements de courte durée ou annuels.	www.thesmallbusinessexpo.com www.makerfaire.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Crypto-monnaie	cryp	1111	Courtages en ligne et sites Web permettant aux utilisateurs d'échanger des crypto-monnaies; informations concernant les crypto-monnaies, notamment analyses, commentaires, conseils, indices de performance et graphiques de cours. Informations générales sur le cryptominage et les entreprises de minage sont incluses dans cette catégorie, mais les domaines et les adresses IP directement impliqués dans les activités de minage sont classés dans la catégorie Cryptominage.	www.coinbase.com www.coinsutra.com
Cryptominage	mine	1112	Hôtes qui participent activement à un pool de minage de crypto-monnaie.	www.give-me-coins.com www.slushpool.com
Sites de rencontres	date	1055	Rencontres, rencontres en ligne, agences matrimoniales.	www.eharmony.com www.match.com
Cartes postales numériques	carte	1082	Envoi de cartes postales numériques et de cartes électroniques.	www.hallmarkecards.com www.bluemountain.com
Restauration et débit de boisson	nourr	1061	Établissements de restauration et débits de boisson; restaurants, bars, tavernes et pubs; guides et critiques gastronomiques.	www.zagat.com www.experiencethepub.com
Projets de Bricolage	bricol	1097	Conseils et informations pour créer, rénover, modifier, décorer et réparer des choses sans faire appel à des experts ou des professionnels.	www.diy-tips.co.uk www.thisoldhouse.com
Tunnellisation DNS	tunn	1122	Sites qui fournissent la tunnellisation DNS en tant que service. Ces services peuvent être destinés à un ordinateur ou à un appareil mobile et créer une connexion VPN spécifiquement sur DNS pour envoyer un trafic qui peut contourner les politiques et les contrôles de l'entreprise.	

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
DoH et DoT	doht	1113	Demandes DNS chiffrées à l'aide du protocole DNS sur HTTPS (DoH) ou DNS sur TLS. Ces protocoles sont généralement utilisés comme couche de sécurité et de confidentialité par les utilisateurs finaux, mais le chiffrement masque la destination de la demande et la fait passer par un tiers.	www.cloudflare-dns.com www.dns.google.com
Dynamique et résidentiel	dyn	1091	Adresses IP des liaisons haut débit qui indiquent généralement que les utilisateurs tentent d'accéder à leur réseau domestique, par exemple pour une session à distance sur un ordinateur personnel.	http://109.60.192.55
Fournisseur de DNS dynamique	ddns	1114	Il est possible d'utiliser les services DNS dynamiques pour rendre certaines applications ou certains contenus accessibles sur le Web à partir de points d'accès hébergés sur des adresses IP attribuées dynamiquement. L'accès est accordé par l'intermédiaire d'un nom d'hôte sur le domaine appartenant au service DNS dynamique.	www.noip.com www.afraid.org
Éducation	édu	1001	Liés à l'éducation, comme les écoles, collèges, universités, matériel pédagogique et ressources pour les enseignants; formation technique et professionnelle; formation en ligne; questions et politiques éducatives; aide financière; financement des écoles; normes et tests.	www.education.com www.greatschools.org
et de	ent	1093	Détails ou discussion de films; musique et groupes; télévision; sites Web de célébrités et de fans; actualités de l'industrie du divertissement; potins; salles de divertissement. Comparez avec la catégorie « Arts ».	www.eonline.com www.ew.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Extreme	extr	1075	Contenus de nature sexuellement violente ou criminelle; violence et comportement violent; photographies de mauvais goût, souvent sanglantes, comme les photos d'autopsies; photos de scènes de crime, de victimes de crimes et d'accidents; contenus excessivement obscènes; sites de choc.	www.car-accidents.com www.crime-scene-photos.com
Mode	mod	1076	Vêtements et mode; salons de coiffure; produits de beauté; accessoires; bijoux; parfum; images et textes relatifs à la modification du corps; tatouages et piercings; agences de mannequins. Les produits dermatologiques sont classés dans la catégorie « Santé et médecine ».	www.fashion.net www.styleseat.com
Services de transfert de fichiers	fts	1071	Services de transfert de fichiers dont le but principal est de fournir des services de téléchargement et de partage de fichiers hébergés	www.sharefile.com www.wetransfer.com
Contournement des filtres	filt	1025	Promotion et assistance pour l'utilisation indétectable et anonyme du Web, notamment services de proxy anonymes cgi, php et glype.	www.bypassschoolfilter.com www.filterbypass.com
Financement	fnnc	1015	Principalement de nature financière, comme les pratiques comptables et les comptables, la fiscalité, les impôts, la banque, les assurances, les investissements, l'économie nationale, les finances personnelles impliquant des assurances de tous types, les cartes de crédit, la retraite et la planification successorale, les prêts, les hypothèques. Les actions et les valeurs mobilières sont classées dans la catégorie « Bourse en ligne ».	www.finance.yahoo.com www.bankofamerica.com
Gratuiciels et partagiciels	gratuit	1068	Offre de téléchargements de logiciels gratuits et en partagiciels.	www.freewarehome.com www.filehippo.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Jeux d'argent	pari	1049	Casinos et jeux d'argent en ligne; bookmakers et cotes; conseils en matière de jeux de hasard; courses de compétition dans un contexte de jeux d'argent; réservations sportives; paris sportifs; services de paris sur la variation des cours boursiers et des actions. Les sites Web portant sur la dépendance au jeu sont classés dans la catégorie « Santé et Médecine ». Les loteries gérées par le gouvernement sont classées comme des « loteries ».	www.888.com www.gambling.com
Jeux	jeu	1007	Divers jeux de cartes, jeux de société, jeux de mots et jeux vidéo; jeux de combat; jeux sportifs; jeux téléchargeables; critiques de jeux; aide-mémoire; jeux informatiques et jeux Internet, tels que jeux de rôle.	www.games.com www.shockwave.com
Gouvernement et droit	gouv	1011	Sites Web gouvernementaux; relations étrangères; actualités et informations relatives au gouvernement et aux élections; informations relatives au domaine du droit, telles que les avocats, les cabinets d'avocats, les publications juridiques, les documents de référence juridiques, les tribunaux, les dossiers et les associations juridiques; législation et décisions de justice; questions de droits civiques; immigration; brevets et droits d'auteur; informations relatives aux systèmes d'application de la loi et correctionnels; signalement d'actes délictuels, application de la loi et statistiques relatives à la criminalité; militaire, comme les forces armées, les bases militaires, les organisations militaires; anti-terrorisme.	www.usa.gov www.law.com
Piratage informatique	pirat	1050	Discussion sur les moyens de contourner la sécurité des sites Web, des logiciels et des ordinateurs.	www.hackthissite.org www.gohacking.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Discours de haine	haine	1016	Sites Web promouvant la haine, l'intolérance ou la discrimination sur la base du groupe social, de la couleur, de la religion, de l'orientation sexuelle, du handicap, de la classe sociale, de l'origine ethnique, de la nationalité, de l'âge, du sexe, de l'identité de genre; sites faisant la promotion du racisme; sexisme; théologie raciste; musique de haine; organisations néonazies; suprémacisme; négation de l'Holocauste.	www.kkk.com www.aryanunity.com
Santé et médecine	sméd	1104	Soins de santé; maladies et handicaps; soins médicaux; hôpitaux; médecins; médicaments; santé mentale; psychiatrie; pharmacologie; exercice et forme physique; handicaps physiques; vitamines et suppléments; sexe dans le contexte de la santé (maladie et soins de santé); tabagisme, alcoolisme, toxicomanie et addiction au jeu dans le contexte de la santé (maladie et soins de santé).	www.webmd.com www.health.com
Humour	lol	1079	Blagues, sketchs, bandes dessinées et autres contenus humoristiques. L'humour adulte susceptible d'offenser est classé dans la catégorie « Adultes ».	www.pun.me www.jokes.com
Chasse	chas	1022	Chasse et pêche, chasse professionnelle ou sportive; clubs de tir et autres sites liés à la chasse.	www.bulletsafaris.com www.mfha.org
Activités illégales	acil	1022	Promotion de la délinquance, telle que le vol, la fraude, l'accès illégal aux réseaux téléphoniques; virus informatiques; terrorisme, bombes et anarchie; sites Web décrivant des meurtres et des suicides et expliquant les moyens de les commettre.	www.ekran.no www.pyrobin.com
Téléchargements illégaux	tlil	1084	Offre la possibilité de télécharger des logiciels ou d'autres contenus, des numéros de série, des générateurs de clés et des outils permettant de contourner la protection des logiciels en violation des accords de droits d'auteur. Les flux de données sont classés dans la catégorie « Transfert de fichiers homologues ».	www.keygenninja.com www.rootscrack.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Drogues illégales	drogue	1047	Informations sur les drogues récréatives, les accessoires liés à la drogue, l'achat et la fabrication de drogues.	www.shroomery.org www.hightimes.com
Réseaux d'infrastructure et de diffusion de contenu	infr	1018	Infrastructure de diffusion de contenu et contenu généré dynamiquement; sites Web qui ne peuvent pas être classés plus spécifiquement parce qu'ils sont sécurisés ou difficiles à classer.	www.akamai.net www.webstat.net
Internet des objets	iot	1116	Domaines utilisés pour surveiller l'état général, l'activité ou aider à la configuration de l'Internet des objets (IoT) et d'autres appareils électroniques compatibles réseau. De plus, ces sites peuvent fournir des mises à jour de logiciels ou de micrologiciels ou permettre un accès à distance pour administrer l'appareil. L'IoT existe à la fois dans les segments grand public et professionnel, dans des produits tels que les imprimantes, les téléviseurs, les thermostats, la supervision des systèmes, l'automatisation et les appliances intelligentes.	www.samsungotn.net www.transport.nest.com
Téléphonie par Internet	VoIP	1067	Services téléphoniques utilisant Internet.	www.skype.com www.getvoca.com
Recherche d'emploi	job (tâche)	1004	Conseils de carrière; compétences en matière de rédaction de CV et d'entrevues; services de placement; banques de données sur les emplois; agences de travail à durée indéterminée et temporaire; sites Web d'employeurs.	www.careerbuilder.com www.monster.com
Lingerie et vêtements de plage	ling	1031	Vêtements intimes et maillots de bain, en particulier mannequinat.	www.swimsuits.com www.victoriassecret.com
Loteries	lotr	1034	Tirages au sort, concours et loteries parrainées par l'État.	www.calottery.com www.flalottery.com
Militaire	mil	1099	Militaire, comme les forces armées; bases militaires; organisations militaires; anti-terrorisme.	www.goarmy.com www.todaysmilitary.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Téléphones cellulaires	cell	1070	Services de messages courts (SMS); sonneries et téléchargements pour téléphones cellulaires. Les sites Web des opérateurs de téléphonie mobile sont inclus dans la catégorie « Entreprise et industrie ».	www.cbfsms.com www.zedge.net
Musées	musé	1117	Musées et expositions, tant en ligne que physiques, dédiés à la préservation d'informations sur des sujets pouvant être d'intérêt général ou hautement spécialisés. Les sujets peuvent aller de l'art à l'histoire, en passant par les sciences ou ils peuvent avoir une importance culturelle.	www.ushmm.org www.louvre.fr
Nature et conservation	ncon	1106	Sites liés aux ressources naturelles; écologie et conservation; forêts; région sauvage; plantes; fleurs; conservation des forêts; pratiques forestières, sauvages et forestières; gestion forestière (reboisement, protection des forêts, conservation, récolte, santé des forêts, éclaircie et brûlage dirigé); pratiques agricoles (agriculture, jardinage, horticulture, aménagement paysager, plantation, contrôle des mauvaises herbes, irrigation, taille et récolte); problèmes de pollution (qualité de l'air, déchets dangereux, prévention de la pollution, recyclage, gestion des déchets, qualité de l'eau et industrie du nettoyage de l'environnement).	www.nature.org www.thepottedgarden.co.uk
Nouveautés	actualités	1058	Nouvelles; gros titres; journaux; chaînes de télé; revues; météo; conditions de ski.	www.cnn.com www.news.bbc.co.uk
Organisations non-gouvernementales	ong	1087	Organisations non gouvernementales telles que clubs, lobbys, communautés, organisations à but non lucratif et syndicats.	www.panda.org www.unions.org
Nudité non sexuelle	nsn	1060	Nudisme et nudité; naturisme; camps nudistes; nus artistiques.	www.1001fessesproject.com www.naturistsociety.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Non exploitable	nexpl	1103	Sites qui ont été inspectés mais sont inaccessibles ou n'ont pas suffisamment de contenu pour se voir attribuer une catégorie.	—
Communautés en ligne	comm	1024	Groupes d'affinité; groupes d'intérêt spéciaux; groupes de discussion Web; babillards électroniques. Exclut les sites Web classés comme « Réseaux professionnels » ou « Réseaux sociaux ».	www.reddit.com www.stackexchange.com
Partage de documents en ligne et collaboration	docs	1115	Logiciels en nuage utilisés pour créer, convertir ou modifier des documents. Les fonctionnalités de collaboration et de partage peuvent être disponibles avec des autorisations d'accès généralement configurées par l'auteur. Les documents peuvent être stockés en ligne ou disponibles en téléchargement.	www.pastebin.com www.docs.google.com
Réunions en ligne	réun	1100	Réunions en ligne; partage de bureau; accès à distance et autres outils facilitant la collaboration multisite	www.join.me www.teamviewer.com
Stockage et sauvegarde en ligne	osb	1066	Stockage hors site et entre homologues pour la sauvegarde, le partage et l'hébergement.	www.adrive.com www.dropbox.com
Bourse en ligne	bours	1028	Courtages en ligne; sites Web permettant à l'utilisateur de négocier des actions en ligne; informations relatives au marché boursier, aux actions, aux obligations, aux fonds communs de placement, aux courtiers, à l'analyse et aux commentaires boursiers, aux écrans boursiers, aux graphiques boursiers, aux introductions en bourse, aux fractionnements d'actions. Les services de paris sur la variation des cours boursiers et des actions sont classés comme des « Jeux de hasard ». Les autres services financiers sont classés dans la catégorie « Finance ».	www.tdameritrade.com www.etrade.com
Courriel organisationnel	pem	1085	Sites Web utilisés pour accéder à la messagerie professionnelle (souvent par le biais d'Outlook Web Access).	www.mail.zoho.com www.webmail.edmc.edu

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Paranormal	prnm	1101	Ovnis; fantômes; cryptide; télékénèse; légendes urbaines; mythes.	www.ghoststudy.com www.ufocasebook.com
Domaines en faux appel	parc	1092	Sites Web qui monétisent le trafic de domaine à l'aide de listes payantes provenant d'un réseau publicitaire ou qui appartiennent à des « squatteurs » dans l'espoir de vendre le nom de domaine dans un but lucratif. Ceux-ci incluent également de faux sites Web de recherche qui renvoient des liens publicitaires payants.	www.domainzaar.com www.cricketbuzz.com
Transfert de fichiers entre homologues	p2p	1056	Sites Web de demande de fichiers entre homologues. Cette catégorie ne suit pas les transferts de fichiers proprement dits.	www.bittorrent.com www.torrentdownloads.me
Sites personnels	pers	1081	Sites Web concernant et émanant de particuliers; serveurs de pages d'accueil personnelles; sites Web présentant des contenus personnels; blogs personnels sans thème particulier.	www.blogmaverick.com www.stallman.org
VPN personnel	pvpn	1102	Sites ou outils de réseaux privés virtuels (VPN) qui sont généralement destinés à un usage personnel et qui peuvent ou non être approuvés pour un usage professionnel.	www.openvpn.net www.torvpn.com
Recherche de photos et d'images	image	1090	Facilitation du stockage et de la recherche d'images, de photographies et d'illustrations.	www.flickr.com www.photobucket.com
Politique	pol	1083	Sites Web politiques; partis politiques; actualités et informations sur la politique, élections, démocratie et vote.	www.politics.com www.gp.org
Pornographie	porno	1054	Texte ou représentations sexuellement explicites. Inclut anime et dessins animés explicites; représentations générales explicites; autres contenus fétichistes; salons de discussion explicites; simulateurs sexuels; strip poker; films pour adultes; art obscène; courrier électronique explicite en ligne.	www.redtube.com www.youporn.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Adresses IP privées comme hôte	piah	1121	Adresses IP privées utilisées comme partie hôte d'une URL. Les adresses IP privées sont destinées à un usage interne uniquement derrière les routeurs frontaliers, elles ne sont donc pas routables publiquement.	
Réseaux professionnels	résp	1089	Réseaux sociaux destinés aux carrières ou au développement professionnel. Voir également « Réseaux sociaux ».	www.linkedin.com www.europeanpwn.net
Immobilier	immo	1045	Informations susceptibles de soutenir la recherche de biens immobiliers; bureaux et espaces commerciaux; annonces immobilières, p. ex. locations, appartements et maisons; construction de maisons.	www.realtor.com www.zillow.com
Recettes et alimentation	rece	1105	Sites dédiés à la discussion sur et au partage d'informations gastronomiques, recettes et aliments ou boissons non alcoolisées; aspects culturels de la cuisine et de l'alimentation; descriptions de régimes et conseils d'observance, informations nutritionnelles générales sur les aliments. Utilisation et instructions sur les appareils et ustensiles de cuisine. Blogs de célébrités du monde culinaire, style de vie et passionnés.	www.allrecipes.com www.seriouseats.com
Numéro de référence	réf	1017	Guides de ville et d'État; cartes, heure; sources de référence; dictionnaires; bibliothèques.	www.wikipedia.org www.yellowpages.com
Sites régionaux restreints (Allemagne)	xdeu	1125	URL restreintes en Allemagne en raison de contenus potentiellement illégaux déterminés par le gouvernement régional.	
Sites régionaux restreints (Grande-Bretagne)	xgbr	1123	URL restreintes en Grande-Bretagne en raison d'un contenu susceptible d'être illégal, tel que déterminé par le gouvernement régional.	
Sites régionaux restreints (Italie)	xita	1124	URL restreintes en Italie en raison d'un contenu susceptible d'être illégal, tel que déterminé par le gouvernement régional.	

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
Sites régionaux restreints (Pologne)	xpol	1126	URL restreintes en Pologne en raison d'un contenu susceptible d'être illégal, tel que déterminé par le gouvernement régional.	www.betsafe62.com www.tornadobet69.com
Religion	rel	1086	Contenus religieux, informations sur les religions; communautés religieuses.	www.religionfacts.com www.religioustolerance.org
Logiciels-services (SaaS) et B2B	saas	1080	Portails Web pour services commerciaux en ligne; réunions en ligne.	www.netsuite.com www.salesforce.com
Sans danger pour les enfants	enfants	1057	Destiné et spécifiquement approuvé pour les jeunes enfants.	www.discoverykids.com www.nickjr.com
Science et technologie	sci	1012	Sciences et technologies, p. ex. aérospatial, électronique, ingénierie, mathématiques et autres matières similaires; exploration de l'espace; météorologie; géographie; environnement; énergie (fossile, nucléaire, renouvelable); communications (téléphones, télécommunications).	www.physorg.com www.science.gov
Portails et moteurs de recherche	rech	1020	Moteurs de recherche et autres premiers points d'accès à l'information sur Internet.	www.bing.com www.google.com
Éducation sexuelle	édsx	1052	Sites Web factuels traitant du sexe; santé sexuelle; contraception; grossesse.	www.avert.org www.scarleteen.com
Magasinage	achat	1005	Troc; achats en ligne; coupons et offres gratuites; fournitures de bureau générales; catalogues en ligne; centres commerciaux en ligne.	www.amazon.com www.shopping.com
Réseaux sociaux	réss	1069	Réseaux sociaux Voir également « Réseaux professionnels ».	www.facebook.com www.twitter.com
Sciences sociales	ssoc	1014	Sciences et histoire liées à la société; archéologie; anthropologie; études culturelles; histoire; linguistique; géographie; philosophie; psychologie; études de femmes.	www.archaeology.org www.anthropology.net
Société et culture	scté	1010	Famille et relations; origine ethnique; organismes sociaux; généalogie; personnes âgées; garde d'enfants.	www.childcareaware.org www.familysearch.org

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
des mises à jour de logiciels	mjlog	1053	Sites Web qui hébergent les mises à jour de logiciels.	www.softwarepatch.com www.windowsupdate.com
Sports et divertissements	sprt	1008	Tous sports, professionnels et amateurs; activités récréatives; pêche; sports fictifs; parcs publics; parcs d'attractions; parcs aquatiques; parc thématiques; zoos et aquariums; spas.	www.espn.com www.recreation.gov
Diffusion audio en continu	aud	1073	Diffusion en continu en temps réel de contenus audio, y compris radio Internet et flux audio.	www.live-radio.net www.shoutcast.com
Lecture vidéo en continu	vid	1072	Diffusion de vidéo en continu et en temps réel, y compris télévision sur Internet, diffusions Web et partage de vidéos.	www.hulu.com www.youtube.com
Terrorisme et extrémisme violent	terr	1119	Sites Web terroristes ou extrémistes à caractère idéologique qui font la promotion de la mort ou de la violence. Les sites peuvent contenir des images, des vidéos et du texte choquants ou perturbateurs. Certains sites peuvent ne pas faire la promotion du terrorisme, mais partager des documents de première main de nature violente.	
Tabac	tab	1078	Sites Internet pro-tabac; fabricants de tabac; pipes et produits pour fumer (non commercialisés pour l'usage de drogues illégales). Le tabagisme est classé dans la catégorie « Santé et médecine ».	www.bat.com www.tobacco.org
Transport	trns	1044	Transport personnel; renseignements concernant les voitures et les deux-roues; achat de voitures et de motos neuves et d'occasion; clubs automobiles; bateaux, avions, véhicules récréatifs (VR) et autres articles similaires. Remarque : les courses de voitures et de deux-roues sont classées dans la catégorie « Sports et divertissements ».	www.cars.com www.motorcycles.com

URL Category (Catégorie URL)	Abréviation	Code	Description	Exemples d'URL
de	trvl	1046	Déplacements professionnels et personnels; renseignements de voyage; ressources de voyage; agents de voyages; forfaits vacances; croisières; logement et hébergement; transport de voyage; réservation de vol; tarifs aériens; location de voiture; maisons de vacances.	www.expedia.com www.lonelyplanet.com
Raccourcisseurs d'URL	raccourci	1120	Domaines utilisés pour raccourcir les URL longues, les URL de marque ou peuvent masquer la destination finale d'un lien hypertexte.	www.bit.ly www.tinyurl.com
Armes	arm	1036	Renseignements relatifs à l'achat ou à l'utilisation d'armes conventionnelles, p. ex. vendeurs d'armes, ventes aux enchères d'armes, petites annonces portant sur les armes à feu, accessoires d'armes à feu, salons d'armes à feu et formation aux armes à feu; informations générales sur les armes à feu; d'autres sites de recherche sur les armes et graphiques peuvent être inclus. Les sites Web militaires du gouvernement sont classés dans la catégorie « Gouvernement et droit ».	www.coldsteel.com www.gunbroker.com
Cache Web et archives	cach	1108	Contenu Web mis en cache ou archivé, souvent stocké à des fins de préservation ou pour réduire les temps de chargement.	www.archive.org www.webcache.googleusercontent.com
Hébergement Web	hébw	1037	Hébergement de sites Web; services de bande passante.	www.bluehost.com www.godaddy.com
Traduction de pages Web	trad	1063	Traduction de pages Web d'une langue à l'autre.	www.babelfish.com www.translate.google.com
Courriel Web	mail	1038	Services de courriel publics sur le Web. Les sites Web permettant aux individus d'accéder au service de messagerie de leur entreprise ou organisation sont classés dans la catégorie « E-mail organisationnel ».	www.mail.yahoo.com www.outlook.com

Thèmes connexes

- Gestion des mises à jour de l'ensemble de catégories d'URL , on page 195
- Signalisation des URL non classées et mal classées, on page 193

CHAPITRE 10

Créer des politiques pour contrôler les demandes Internet

Cette rubrique contient les sections suivantes :

Présentation des politiques : contrôler les demandes Internet interceptées

Lorsque l'utilisateur crée une demande Web, le Secure Web Appliance configuré intercepte les demandes et gère le processus dont la demande parcourt pour arriver à son résultat final, qu'il s'agisse d'accéder à un site Web particulier, à un courriel ou même à une application en ligne. Lors de la configuration de Secure Web Appliance des politiques sont créées pour définir les critères et les actions des demandes faites par l'utilisateur.

Les politiques sont les moyens par lesquels Secure Web Appliance identifie et contrôle les demandes Web. Lorsqu'un client envoie une demande Web à un serveur, le proxy Web reçoit la demande, l'évalue et détermine à quelle politique elle appartient. Les actions définies dans la politique sont ensuite appliquées à la demande.

Secure Web Appliance utilise plusieurs types de politiques pour gérer différents aspects des demandes Web. Les types de politiques peuvent gérer entièrement les transactions par eux-mêmes ou transmettre les transactions à d'autres types de politiques pour un traitement supplémentaire. Les types de politiques peuvent être regroupés en fonction des fonctions qu'ils remplissent, comme l'accès, le routage ou la sécurité.

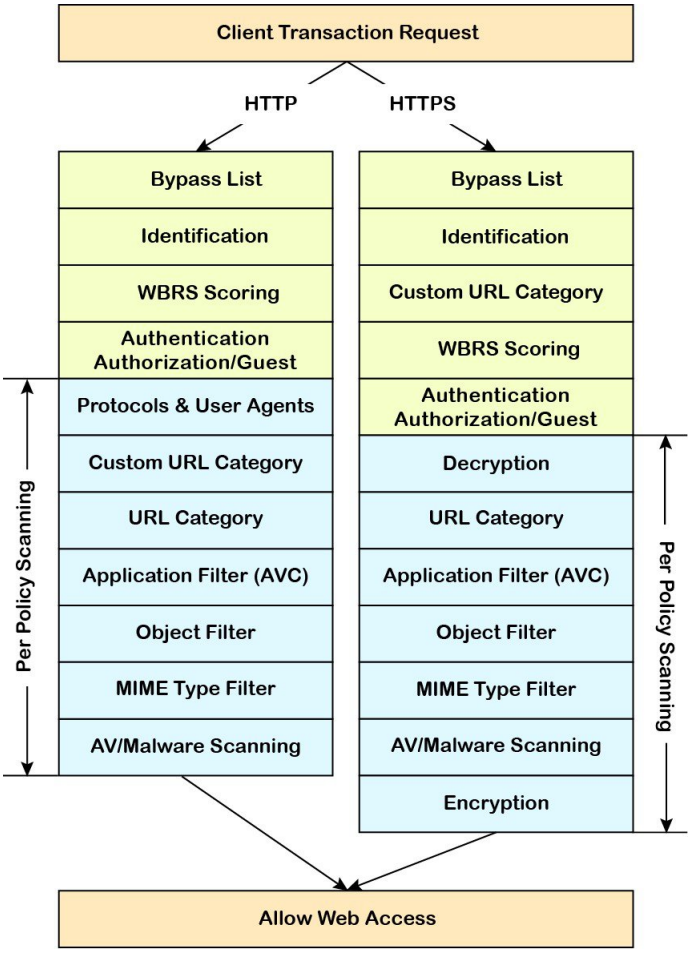
AsyncOS évalue les transactions en fonction des politiques avant d'évaluer les dépendances externes pour éviter toute communication externe inutile de l'appliance. Par exemple, si une transaction est bloquée en

fonction d'une politique qui bloque les URL non classées, la transaction n'échouera pas en fonction d'une erreur DNS.

Traitement des demandes HTTP/HTTPS interceptées

Le diagramme suivant décrit le flux d'une demande Web interceptée lors de son traitement par l'appliance.

Figure 3: Flux de transaction HTTP/HTTPS



Consultez également les diagrammes suivants qui représentent les divers flux de traitement des transactions :

- Figure 1: Profils d'identification et traitement d'authentification – Aucune substitution et substitutions basées sur IP, on page 162
- Figure 2: Profils d'identification et traitement d'authentification – Substitutions basées sur des témoins, on page 163
- Figure 4: Flux des transactions de groupe des politiques d'accès, on page 253
- Figure 7: Flux de transaction des groupes de politiques pour les politiques de déchiffrement, on page 283
- Contrôle du trafic HTTPS, on page 285

Présentation des tâches de gestion des demandes Web au moyen de politiques

Étape	Liste des tâches pour la gestion des demandes Web au moyen des politiques	Liens vers des rubriques et des procédures connexes
1	Configurer et séquencer les domaines d'authentification	Domaines d'authentification, on page 115
2	(Pour les proxy en amont) Créez un groupe de proxy.	Création de groupes de serveurs proxy pour les serveurs proxy en amont, on page 25
2	(Facultatif) Créer des applications clientes personnalisées	Applications client, on page 267
3	(Facultatif) Créer des catégories d'URL personnalisées	Création et modification de catégories d'URL personnalisées, on page 211
4	Créer des profils d'identification	Classification des utilisateurs et logiciels clients, on page 153
5	(Facultatif) Créer des plages de temps pour limiter l'accès en fonction de l'heure	Plages de temps et quotas, on page 269
6	Créer et trier des politiques	• Création d'une politique , on page 253 • Ordre des politiques, on page 252

Bonnes pratiques en matière de gestion des demandes Web au moyen de politiques

Si vous souhaitez utiliser les objets utilisateur Active Directory pour gérer les demandes Web, n'utilisez pas les groupes principaux comme critères. Les objets utilisateur Active Directory ne contiennent pas de groupe principal.

Politiques

- Types de politique, on page 250
- Ordre des politiques, on page 252
- Création d'une politique , on page 253

Types de politique

Type de politique	Type de requête	Description	Lien vers la tâche
Accès	• HTTP • HTTPS déchiffré • FTP	Bloquer, autoriser ou rediriger le trafic HTTP, FTP et HTTPS déchiffré entrant. Les politiques d'accès gèrent également le trafic HTTPS chiffré entrant si le proxy HTTPS est désactivé.	Création d'une politique , on page 253
SOCKS	• SOCKS	Autorisez ou bloquez les demandes de communication SOCKS.	Création d'une politique , on page 253
Authentification de l'application	• application	Autorisez ou refusez l'accès à un logiciel-service (SaaS). Utilisez la connexion unique pour authentifier les utilisateurs et renforcer la sécurité en permettant de désactiver rapidement l'accès aux applications. Pour utiliser la fonctionnalité de connexion unique des politiques, vous devez configurer Secure Web Appliance comme fournisseur d'identité et charger ou générer un certificat et une clé pour le logiciel-service.	Création de politiques d'authentification d'applications de logiciel-service (SaaS), on page 168
Gestion du protocole HTTPS chiffré	• HTTPS	Déchiffrez, transmettez ou abandonnez les connexions HTTPS. AsyncOS transmet le trafic déchiffré aux politiques d'accès pour traitement ultérieur.	Création d'une politique , on page 253
Sécurité des données	• HTTP • HTTPS déchiffré • FTP	Gérez les chargements de données sur le Web. Les politiques de sécurité des données analysent le trafic sortant pour s'assurer qu'il est conforme aux règles de l'entreprise pour les téléchargements de données, en fonction de sa destination et de son contenu. Contrairement aux politiques DLP externes, qui redirigent le trafic sortant vers des serveurs externes pour l'analyse, les politiques de sécurité des données utilisent Secure Web Appliance pour analyser et évaluer le trafic.	Création d'une politique , on page 253

Type de politique	Type de requête	Description	Lien vers la tâche
DLP (Data Loss Prevention) externe	• HTTP • HTTPS déchiffré • FTP	Envoyez le trafic sortant vers des serveurs exécutant des systèmes DLP tiers, qui l'analysent pour vérifier le respect des règles de l'entreprise pour le chargement de données. Contrairement aux politiques de sécurité des données, qui gèrent également les téléchargements de données, les politiques DLP externes déplacent le travail d'analyse loin de Secure Web Appliance, ce qui libère des ressources sur l'appliance et exploite toutes les fonctionnalités supplémentaires offertes par les logiciels tiers.	Création d'une politique , on page 253
Analyse des programmes malveillants sortants	• HTTP • HTTPS déchiffré • FTP	Bloquer, surveiller ou autoriser les demandes de téléchargement de données susceptibles de contenir des données malveillantes. Empêchez la transmission des programmes malveillants déjà présents sur votre réseau à des réseaux externes.	Création d'une politique , on page 253
Routage	• HTTP • HTTPS • FTP	Faites passer le trafic Web par des proxy en amont ou vers des serveurs de destination. Vous souhaiterez peut-être rediriger le trafic vers des proxys en amont pour préserver la conception de votre réseau existante, pour décharger le traitement de Secure Web Appliance, ou pour tirer parti des fonctionnalités supplémentaires fournies par les systèmes proxy tiers. Si plusieurs proxys en amont sont disponibles, Secure Web Appliance peut utiliser des techniques d'équilibrage de la charge pour leur distribuer des données. Conservez l'adresse IP source du client, remplacez-la par l'adresse IP du proxy Web ou une adresse IP personnalisée à l'aide du profil d'espionnage IP.	Création d'une politique , on page 253

Chaque type de politiques utilise un tableau de politiques pour stocker et gérer ses politiques. Chaque tableau de politique est accompagné d'une politique globale prédéfinie, qui conserve les actions par défaut pour un type de politique. Des politiques supplémentaires définies par l'utilisateur sont créées et ajoutées au tableau de politiques le cas échéant. Les politiques sont traitées dans l'ordre dans lequel elles sont répertoriées dans le tableau des politiques.

Les politiques individuelles définissent les types de demandes des utilisateurs qu'elles gèrent et les actions qu'elles effectuent sur ces demandes. Chaque définition de politique comporte deux sections principales :

- **Profils d'identification et utilisateurs** : Les profils d'identification sont utilisés dans les critères d'appartenance à la politique et sont particulièrement importants car ils contiennent de nombreuses options pour identifier les transactions Web. Ils partagent également de nombreuses propriétés avec les politiques.
- **Niveau avancé** : critères utilisés pour identifier les utilisateurs auxquels la politique s'applique. Un ou plusieurs critères peuvent être précisés dans une politique, et tous doivent correspondre pour que les critères soient remplis.
  - **Protocoles** : permettent le transfert de données entre divers périphériques de réseau comme http, https, ftp, etc.
  - **Ports de proxy** : port numéroté par lequel la demande accède au proxy Web,
  - **Sous-réseaux** : le regroupement logique des périphériques réseau connectés [comme l'emplacement géographique ou le réseau local (LAN)], d'où provient la demande
  - **Plage de temps** : des plages de temps peuvent être créées pour être utilisées dans les politiques afin d'identifier ou d'appliquer des actions aux demandes Web en fonction de l'heure ou du jour où les demandes ont été effectuées. Les plages de temps sont créées en tant qu'unités individuelles.
  - **Catégories d'URL** : les catégories d'URL sont des catégories prédéfinies ou personnalisées de sites Web, tels que les actualités, les affaires, les médias sociaux, etc. Elles peuvent être utilisées pour identifier ou appliquer des actions aux demandes Web.
  - **Agents utilisateurs** : Il s'agit des applications client (comme les programmes de mise à jour et les navigateurs Web) utilisées pour formuler des demandes. Vous pouvez définir des critères de politique basés sur les agents utilisateurs et vous pouvez spécifier des paramètres de contrôle basés sur les agents utilisateurs. Vous pouvez également dispenser les agents utilisateurs de l'authentification, ce qui est utile pour les applications qui ne peuvent pas demander des informations d'authentification. Vous pouvez définir des agents utilisateurs personnalisés, mais vous ne pouvez pas réutiliser ces définitions dans d'autres politiques.

Note Lorsque vous définissez plusieurs critères d'appartenance, la demande du client doit satisfaire à tous les critères pour correspondre à la politique.

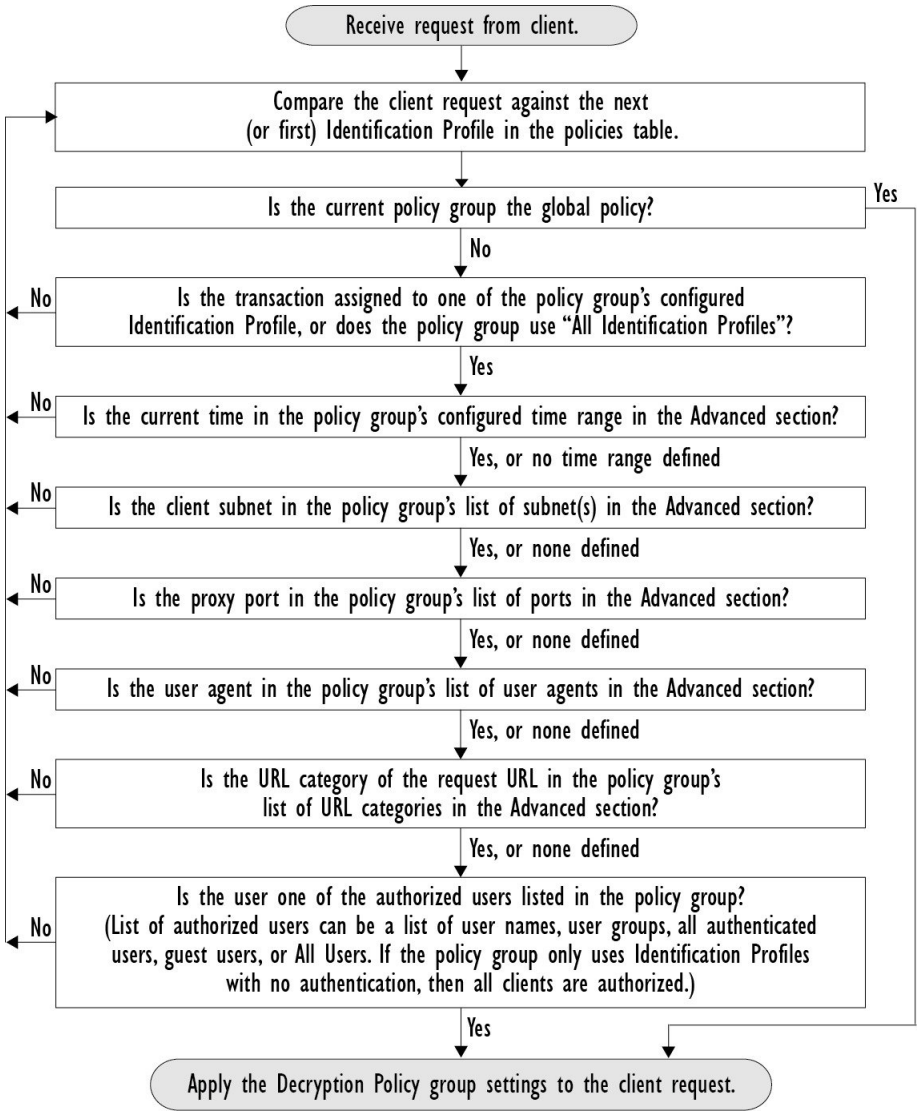
Ordre des politiques

L'ordre dans lequel les politiques sont répertoriées dans un tableau détermine la priorité avec laquelle elles sont appliquées aux demandes Web. Les demandes Web sont vérifiées par rapport aux politiques en commençant en haut du tableau jusqu'à la première politique correspondante. Toutes les politiques en dessous de ce point dans le tableau ne sont pas traitées.

Si aucune politique définie par l'utilisateur ne correspond à une demande Web, la politique globale de ce type de politique est appliquée. Les politiques globales sont toujours placées en dernier dans les tableaux et ne peuvent pas être réordonnées.

Le diagramme suivant décrit le flux d'une demande d'un client dans le tableau des politiques d'accès.

Figure 4: Flux des transactions de groupe des politiques d'accès



Création d'une politique

Before you begin

- Activez le proxy approprié :
  - Proxy Web (pour HTTP, HTTPS déchiffré et FTP)
  - Proxy HTTPS

- Proxy SOCKS

- Créez des profils d'identification associés.
- Comprenez Ordre des politiques, on page 252.
- (HTTPS chiffré uniquement) Chargez ou générez un certificat et une clé.
- (Sécurité des données uniquement) Activez les paramètres des filtres de sécurité des données Cisco.
- (DLP externe uniquement) Définissez un serveur DLP externe.
- (Routage uniquement) Définissez le proxy en amont associé sur Secure Web Appliance.
- (Facultatif) Créez des applications clientes associées.
- (Facultatif) Créez des plages de temps associées. Consultez Plages de temps et quotas, on page 269.
- (Facultatif) Créez des catégories d'URL associées. Consultez Création et modification de catégories d'URL personnalisées, on page 211.

Étape 1 Dans la section **Policy Settings** (Paramètres de politique), cochez la case **Enable Identity** (Activer l'identité) pour activer cette politique ou pour la désactiver rapidement sans la supprimer.

Étape 2 Attribuez à la politique un **nom** unique.

Étape 3 La **description** est facultative.

Étape 4 Dans la liste déroulante Insert Above (Insérer au-dessus), choisissez l'emplacement de l'affichage de cette politique dans le tableau.

Note Organisez les politiques de sorte que, de haut en bas du tableau, elles aillent de la plus restrictive à la moins restrictive. Consultez Ordre des politiques, on page 252 pour obtenir de plus amples renseignements.

Étape 5 Dans la zone **Policy Expires** (Expiration de la politique), cochez la case **Set Expiration for Policy** (Définir l'expiration de la politique) pour définir le délai d'expiration de la politique. Saisissez la date et l'heure d'expiration de la politique que vous souhaitez définir. Les politiques sont automatiquement désactivées une fois qu'elles ont dépassé le délai d'expiration défini.

Note Le système vérifie les politiques toutes les minutes pour désactiver celles qui expirent dans la minute. Par exemple, si une politique est configurée pour expirer à 11 h 00, elle sera au maximum désactivée à 11 h 01.

La fonctionnalité d'expiration de politique s'applique uniquement aux politiques d'accès, de déchiffrement et de dérivation du trafic Web.

Vous recevrez un courriel trois jours avant l'expiration du contrat et un autre courriel à l'expiration de la politique.

Note Pour recevoir des alertes, vous devez activer les alertes d'expiration des politiques dans **System Administration** > **Alerts** (Administration système > Alertes). Voir la section Alertes d'expiration des politiques, on page 602.

Vous pouvez également définir le délai d'expiration de la politique à l'aide des appliances Cisco Content Security Management. Les politiques expireront après le délai d'expiration défini, mais ne seront pas affichées comme désactivées dans l'interface graphique utilisateur des appliances Cisco Content Security Management.

Une fois que vous avez défini la fonction d'expiration de la politique, l'expiration se produit en fonction des paramètres d'heure locale de l'appliance.

Étape 6 Dans la section **Policy Member Defined** (Définition des membres de la politique), indiquez la façon dont l'utilisateur et l'appartenance au groupe sont définis : dans la liste Identification Profiles and Users (Profils d'identification et utilisateurs), choisissez l'une des options suivantes :

- **All Identification Profiles** (Tous les profils d'identification) : cette politique s'appliquera à tous les profils existants. Vous devez également définir au moins une option **avancée**.
- **Select One or More Identification Profiles** (Sélectionner un ou plusieurs profils d'identification) : un tableau dans lequel vous pouvez spécifier les profils d'identification individuels s'affiche, une définition de profil d'appartenance par ligne.

Étape 7 Si vous avez choisi **All Identification Profiles** (Tous les profils d'identification) :

a) Indiquez les utilisateurs et les groupes autorisés auxquels cette politique s'applique en sélectionnant l'une des options suivantes :

- **All Authenticated Users** (Tous les utilisateurs authentifiés) : tous les utilisateurs identifiés par authentification ou identification transparente.
- **Selected Groups and Users** (Groupes et utilisateurs sélectionnés) : des utilisateurs et des groupes spécifiés sont utilisés.

  Pour ajouter ou modifier des **étiquettes Groupe sécurisé ISE** et les utilisateurs spécifiés, cliquez sur le lien suivant l'étiquette appropriée. Par exemple, cliquez sur la liste des utilisateurs actuellement spécifiés pour modifier cette liste. Consultez Ajout et modification d'étiquettes Groupe sécurisé pour une politique, on page 257 pour obtenir de plus amples renseignements.

  Si vous utilisez ISE, vous pouvez ajouter ou modifier des étiquettes Groupe sécurisé ISE. Cette fonction n'est pas prise en charge dans les déploiements ISE-PIC. Pour ajouter ou modifier des **groupes ISE** spécifiés, cliquez sur le lien suivant l'étiquette. Cette option est spécifique à ISE-PIC.
- **Guests** (Invités) : utilisateurs connectés en tant qu'invités et utilisateurs dont l'authentification a échoué.
- **All Users** (Tous les utilisateurs) : tous les clients, qu'ils soient authentifiés ou non. Si cette option est sélectionnée, au moins une option **avancée** doit également être définie.

Étape 8 Si vous avez choisi **Select One or More Identification Profiles** (Sélectionner un ou plusieurs profils d'identification), un tableau de sélection de profils s'affiche.

a) Choisissez un profil d'identification dans la liste déroulante Select Identification Profile (Sélectionner un profil d'identification) dans la colonne Identification Profiles (Profils d'identification).

b) Indiquez les utilisateurs et les groupes autorisés auxquels cette politique s'applique :

- **All Authenticated Users** (Tous les utilisateurs authentifiés) : tous les utilisateurs identifiés par authentification ou identification transparente.
- **Selected Groups and Users** (Groupes et utilisateurs sélectionnés) : des utilisateurs et des groupes spécifiés sont utilisés.

  Pour ajouter ou modifier les étiquettes Groupe sécurisé et les utilisateurs spécifiés, cliquez sur le lien suivant l'étiquette appropriée. Par exemple, cliquez sur la liste des utilisateurs actuellement spécifiés pour modifier cette liste. Consultez Ajout et modification d'étiquettes Groupe sécurisé pour une politique, on page 257 pour obtenir de plus amples renseignements.
- **Guests** (Invités) : utilisateurs connectés en tant qu'invités et utilisateurs dont l'authentification a échoué.

c) Pour ajouter une ligne au tableau de sélection de profils, cliquez sur **Add Identification Profile** (Ajouter un profil d'identification). Pour supprimer une ligne, cliquez sur l'icône de corbeille sur cette ligne.

Répétez les étapes (a) à (c) selon les besoins pour ajouter tous les profils d'identification souhaités.

Étape 9 Développez la section **Advanced** (Niveau avancé) pour définir des critères d'appartenance au groupe supplémentaires. [Cette étape peut être facultative selon la sélection dans la section **Policy Member Definition** (Définition des membres d'une politique). En outre, certaines des options suivantes ne seront pas disponibles, selon le type de politique que vous configurez.] .

Option avancée	Description
Protocols (Protocoles)	Sélectionnez les protocoles auxquels cette politique s'appliquera. **All others** (Tous les autres) désigne tout protocole non sélectionné. Si le profil d'identification associé s'applique à des protocoles spécifiques, la présente politique s'applique à ces mêmes protocoles
Proxy Ports (Ports du proxy)	Applique cette politique uniquement au trafic qui utilise des ports spécifiques pour accéder au proxy Web. Saisissez un ou plusieurs numéros de port en séparant les ports par des virgules. Pour les connexions de transfert explicite, il s'agit du port configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination. **Note** Si le profil d'identification associé s'applique uniquement à des ports proxy spécifiques, vous ne pouvez pas saisir ces ports proxy ici.
Subnets (Sous-réseaux)	Applique cette politique uniquement au trafic sur des sous-réseaux spécifiques. Sélectionnez **Define subnets** (Définir des sous-réseaux) et saisissez les sous-réseaux spécifiques, en les séparant par des virgules. Laissez l'option **Use subnets from selected Identities** (Utiliser des sous-réseaux à partir d'identités sélectionnées) si vous ne souhaitez pas de filtrage supplémentaire par sous-réseau. **Note** Si l'identité associée s'applique à des sous-réseaux spécifiques, vous pouvez restreindre davantage l'application de cette politique à un sous-ensemble d'adresses auxquelles l'identité s'applique.
Time Range (Plage de temps)	Vous pouvez appliquer des plages de temps pour l'appartenance à la politique : • Time Range (Plage de temps) : choisissez une plage de temps définie précédemment (Plages de temps et quotas, on page 269). • Match Time Range (Correspondre à la plage de temps) : utilisez cette option pour indiquer si cette plage de temps est inclusive ou exclusive. En d'autres termes, veillez à ce que les données correspondent uniquement à la plage spécifiée ou à tout intervalle hormis la plage spécifiée.
URL Categories (Catégories d'URL)	Vous pouvez restreindre l'appartenance à la politique par destinations (URL) spécifiques et par catégories d'URL. Sélectionnez toutes les catégories personnalisées et prédéfinies souhaitées. Consultez Création et modification de catégories d'URL personnalisées, on page 211 pour en savoir plus sur les catégories personnalisées.

Option avancée	Description

User Agents (Agents utilisateur)	Vous pouvez sélectionner des agents utilisateur spécifiques et définir des agents personnalisés à l'aide d'expressions régulières dans le cadre de la définition de l'appartenance à cette politique.
	• **Common User Agents** (Agents utilisateur communs)
	  • **Browsers** (Navigateurs) : développez cette section pour sélectionner différents navigateurs Web.
	  • **Others** (Autres) : développez cette section pour sélectionner des agents spécifiques autres que les navigateurs, tels que les programmes de mise à jour d'applications.
	• **Custom User Agents** (Agents utilisateur personnalisés) : vous pouvez entrer une ou plusieurs expressions régulières, une par ligne, pour définir des agents utilisateur personnalisés.
	• **Match User Agents** (Correspondre aux agents utilisateur) : utilisez cette option pour indiquer si ces spécifications d'agents utilisateur sont inclusives ou exclusives. Autrement dit, si la définition de l'appartenance inclut uniquement les agents utilisateur sélectionnés ou exclut expressément les agents utilisateur sélectionnés.

Ajout et modification d'étiquettes Groupe sécurisé pour une politique

Pour modifier la liste des étiquettes Groupe sécurisé affectées à un profil d'identification particulier dans une politique, cliquez sur le lien à côté de l'étiquettes Groupe sécurisé ISE dans la liste des groupes et des utilisateurs sélectionnés de la page Add/Edit Policy (Ajouter/modifier une politique). (Consultez Création d'une politique , on page 253.) Ce lien est soit « No tags entered » (Aucune étiquette saisie), soit une liste des étiquettes actuellement attribuées. Le lien ouvre la page Add/Edit Secure Group Tags (Ajouter/modifier des étiquettes Groupe sécurisé).

Toutes les étiquettes Groupe sécurisé actuellement affectées à cette politique sont répertoriées dans la section des étiquettes Groupe sécurisé autorisées. Toutes les balises SGT disponibles sur le serveur ISE connecté sont répertoriées dans la section de recherche des balises SGT.

Étape 1 Pour ajouter une ou plusieurs étiquettes Groupe sécurisé à la liste des étiquettes Groupe sécurisé autorisées, sélectionnez les entrées souhaitées dans la section de recherche d'étiquettes Groupe sécurisé , puis cliquez sur **Add** (Ajouter).

Note
- Les balises SGT déjà ajoutées sont surlignées en vert. Pour trouver rapidement une balise SGT spécifique dans la liste des balises disponibles, entrez une chaîne de texte dans le champ **Search** (Recherche).
- Lorsqu'un Secure Web Appliance est connecté à ISE/ISE-PIC, les balises SGT par défaut d'ISE/ISE-PIC sont également affichées. Aucun utilisateur ne sera affecté à ces balises SGT. Assurez-vous de sélectionner les balises SGT adéquates.

Étape 2 Pour supprimer une ou plusieurs étiquettes Groupe sécurisé de la liste des étiquettes Groupe sécurisé autorisées, sélectionnez ces entrées, puis cliquez sur **Delete** (Supprimer).

Étape 3 Cliquez sur Done (Terminé) pour revenir à la page Add/Edit Group (Add/Modifier un groupe).

What to do next

Thèmes connexes

- Plages de temps et quotas, on page 269
- Utilisation des applications clientes dans les politiques, on page 268

Ajout de la destination de routage et du profil d'usurpation d'adresses IP à la politique de routage

Vous pouvez configurer la manière dont le proxy Web transfère le trafic Web et les demandes à partir de l'adresse IP source en configurant la destination du routage et le profil d'usurpation d'adresses IP dans les politiques de routage.

Note

- La politique de routage globale est activée par défaut même si un groupe de proxys en amont n'est pas configuré sur l'appliance.
- Les profils d'usurpation d'adresses IP ne sont pas liés à la destination de routage et peuvent être configurés indépendamment.
- La politique de routage peut être activée sans configurer un proxy en amont.

Note Pour configurer un groupe de proxy en amont pour une politique de routage dans l'appliance de gestion de la sécurité, enregistrez le fichier de configuration de Secure Web Appliance et importez-le sur l'appliance de gestion de la sécurité. Sinon, l'appliance de gestion de la sécurité affiche le proxy en amont comme «Not Found » (Introuvable) et la politique de routage sera désactivée après l'envoi de la configuration.

Étape 1 Choisissez **Web Security Manager** > **Routing Policies** (Web Security Manager > Politiques de routage).

Étape 2 Dans la page **Routing Policies** (Politiques de routage), cliquez sur le lien sous la colonne **Routing Destination** (Destination de routage) correspondant à la politique de routage que vous souhaitez configurer pour le groupe de proxy en amont.

Étape 3 Choisissez un groupe de proxy en amont approprié parmi les groupes suivants pour la politique sélectionnée :

Action	Description
Use Global Policy Settings (Utiliser les paramètres de la politique globale)	Le proxy Web utilise les paramètres définis dans la politique globale. Il s'agit de l'action par défaut pour les groupes de politiques définies par l'utilisateur. Par défaut, la destination de routage pour la politique de routage globale est renseignée par **Direct Connection** (Connexion directe). S'applique uniquement aux groupes de politiques définies par l'utilisateur.
Direct Connection (Connexion directe)	Le proxy Web transfère le trafic Web directement vers son serveur Web de destination.

Action	Description
Custom upstream proxy group (Groupe de proxy en amont personnalisé)	Le proxy Web redirige le trafic Web vers un groupe de proxy externe en amont. Pour plus d'informations sur la création de groupes de proxy en amont, consultez Serveurs proxy en amont, on page 25.

Étape 4 Dans la page **Routing Policies** (Politiques de routage),cliquez sur le lien sous la colonne **IP Spoofing** (Usurpation d'adresses IP) pour la politique de routage dont vous souhaitez configurer le profil d'usurpation d'adresses IP.

Étape 5 Choisissez un profil d'usurpation d'adresse IP approprié pour la politique sélectionnée parmi les suivantes :

Action	Description
Use Global Policy Settings (Utiliser les paramètres de la politique globale)	Le proxy Web utilise les paramètres définis dans la politique globale. Il s'agit de l'action par défaut pour les groupes de politiques définies par l'utilisateur. Par défaut, l'usurpation d'adresses IP est désactivée pour la politique de routage globale. S'applique uniquement aux groupes de politiques définies par l'utilisateur.
Do No Use IP Spoofing (Ne pas utiliser d'usurpation d'adresses IP)	Le proxy Web modifie l'adresse IP de la source de la demande pour qu'elle corresponde à sa propre adresse afin d'augmenter la sécurité.
Use Client IP (Utiliser l'adresse IP du client)	Le proxy Web conserve l'adresse source de sorte qu'elle semble provenir du client source plutôt que de Secure Web Appliance.
Custom spoofing profile name (Nom de profil d'usurpation personnalisé)	Le proxy Web remplace l'adresse IP de la source de la demande par une adresse IP personnalisée définie dans le nom de profil d'usurpation d'adresses IP personnalisé sélectionné.

Étape 6 **Envoyez** et **validez** vos modifications.

What to do next

Thèmes connexes

- Serveurs proxy en amont, on page 25
- Usurpation d'adresses IP de proxy Web, on page 79

Configuration des politiques

Chaque ligne d'un tableau de politiques représente une définition de politique et chaque colonne de l'affichage actuel contient un lien vers une page de configuration pour cet élément de la politique.

Note Parmi les composants de configuration de politique suivants, vous pouvez spécifier l'option « Warn » (Avertir) uniquement avec le filtrage d'URL.

Option	Description
Protocols and User Agents (Protocoles et agents utilisateur)	Utilisé pour contrôler l'accès aux protocoles et configurer le blocage pour des applications client particulières, telles que les clients de messagerie instantanée, les navigateurs Web et les services de téléphonie sur Internet. Vous pouvez également configurer l'appliance pour tunneliser les demandes HTTP CONNECT sur des ports spécifiques. Lorsque la tunnellisation est activée, l'appliance fait passer le trafic HTTP par des ports spécifiés sans l'évaluer.
URL Filtering (Filtrage URL)	AsyncOS pour le Web vous permet de configurer la façon dont l'appliance gère une transaction en fonction de la catégorie d'URL d'une demande HTTP ou HTTPS particulière. À l'aide d'une liste de catégories prédéfinies, vous pouvez choisir de bloquer, de surveiller, d'alerter ou de définir des filtres basés sur les quotas ou le temps. Vous pouvez également créer des catégories d'URL personnalisées, puis choisir de bloquer, rediriger, autoriser, surveiller, avertir ou appliquer des filtres sur la base de quotas ou du temps pour les sites Web dans les catégories personnalisées. Voir Création et modification de catégories d'URL personnalisées, on page 211 pour plus d'informations sur la création de catégories d'URL personnalisées. En outre, vous pouvez ajouter des exceptions au blocage de contenu intégré ou référencé.
Applications	Le moteur de contrôle et de visibilité des applications (AVC) est un composant de la politique d'utilisation acceptable qui inspecte le trafic Web pour mieux comprendre et contrôler le trafic Web utilisé pour les applications. L'appliance autorise la configuration du proxy Web de manière à bloquer ou autoriser des applications par types d'applications et par application individuelle. Vous pouvez également appliquer des contrôles à des comportements d'applications particuliers, tels que les transferts de fichiers, au sein d'une application particulière. Voir Gestion de l'accès aux applications Web, on page 347 pour les informations de configuration.
Objects (Objets)	Ces options vous permettent de configurer le proxy Web pour bloquer les téléchargements de fichiers en fonction des caractéristiques du fichier, telles que la taille du fichier, le et le type MIME. Un objet est, généralement, tout élément qui peut être sélectionné, chargé, téléchargé et manipulé individuellement. Voir Politiques d'accès : blocage d'objets, on page 262 pour plus d'informations sur la définition d'objets bloqués

Option	Description
Anti-Malware and Reputation (Protection contre les programmes malveillants et réputation)	Les filtres de réputation Web permettent d'affecter un score de réputation de sites Web à une URL afin de déterminer sa probabilité de contenir des programmes malveillants basés sur l'URL. L'analyse de protection contre les programmes malveillants détecte et bloque les menaces de programmes malveillants sur le Web. Cisco Secure Endpoint identifie les programmes malveillants dans les fichiers téléchargés. La politique relative aux programmes malveillants et à la réputation hérite des paramètres globaux respectifs de chaque composant. Dans **Security Services** > **Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation), les catégories de programmes malveillants peuvent être personnalisées de manière à les surveiller ou à les bloquer en fonction des verdicts des analyses des programmes malveillants, et des seuils de score de réputation Web peuvent être personnalisés. Les catégories de programmes malveillants peuvent être personnalisées davantage dans une politique. Il existe également des paramètres globaux pour la réputation des fichiers et les services d'analyse. Pour plus de renseignements, consultez les sections Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès, on page 313 et Configuration des fonctionnalités d'analyse et de réputation de fichiers, on page 328.
HTTP ReWrite Profile (Profil de réécriture HTTP)	Vous pouvez configurer des profils d'en-tête personnalisés pour les requêtes HTTP et créer plusieurs en-têtes dans un profil de réécriture d'en-tête. La fonction de profil de réécriture d'en-tête permet à l'appliance de transmettre les informations sur l'utilisateur et le groupe à un autre périphérique en amont une fois l'authentification réussie. Le proxy en amont considère l'utilisateur comme authentifié, contourne l'authentification supplémentaire et fournit un accès à l'utilisateur en fonction des politiques d'accès définies. Consultez En-têtes personnalisés du proxy Web par politique, on page 83.
Clone Policy (Clonage de politique)	Si une politique existante comporte la plupart des paramètres que vous souhaitez dans une nouvelle politique, vous pouvez gagner du temps en clonant la politique existante, puis en la modifiant. Bien que la politique clonée partage les mêmes attributs de regroupement, elle possède sa propre identité unique, telle que le nom d'affichage, l'adresse IP, l'hôte et le nom de domaine. Les politiques suivantes avec l'option de clonage dans Cisco Secure Web Appliance peuvent également être gérées par Cisco Secure Email and Web Manager (SMA) : • Accès • Déchiffrement • Identification • Routage **Note** Vous ne pouvez copier qu'une seule politique par instance.

Option	Description
Clone Policy (Supprimer)	Supprime la politique créée.

Politiques d'accès : blocage d'objets

Vous pouvez utiliser les options de la page Politiques d'accès : Objets pour bloquer les téléchargements de fichiers en fonction des caractéristiques du fichier, telles que la taille du fichier, le type de fichier et le type MIME. Un objet est, généralement, tout élément qui peut être sélectionné, chargé, téléchargé et manipulé individuellement.

Vous pouvez préciser un certain nombre de types d'objets à bloquer par chaque politique d'accès et par la politique globale. Ces types d'objets comprennent les archives, les types de documents, le code exécutable, le contenu de la page Web, etc.

Étape 1 Dans la page des politiques d'accès [**Web Security Manager** > **Access Policies** (Web Security Manager > Politiques d'accès)], cliquez sur le lien dans la colonne **Objects** (Objets) de la ligne représentant la politique que vous souhaitez modifier.

Étape 2 Choisissez le type de blocage d'objet souhaité pour cette politique d'accès :

- **Use Global Policy Objects Blocking Settings** (Utiliser les paramètres de blocage des objets de politique globale) : cette politique utilise les paramètres de blocage d'objets définis pour la politique globale; ces paramètres sont affichés en mode lecture seule. Modifiez les paramètres de la politique globale pour les modifier.
- **Define Custom Objects Blocking Settings** (Définir les paramètres de blocage d'objets personnalisés) : vous pouvez modifier tous les paramètres de blocage d'objets pour cette politique.
- **Disable Object Blocking for this Policy** (Désactiver le blocage d'objets pour cette politique) : le blocage d'objets est désactivé pour cette politique; aucune option de blocage d'objet ne s'affiche.

Étape 3 Si vous avez choisi **Define Custom Objects Blocking Settings** (Définir les paramètres de blocage des objets personnalisés) à l'étape précédente, activez et désélectionnez les options de blocage d'objets dans la page Access Policies: Objects (Politiques d'accès : Objets), selon vos besoins.

Object Size (Taille de l'objet)	Vous pouvez bloquer des objets en fonction de leur taille de téléchargement : • **Taille maximale de téléchargement HTTP/HTTPS** : indiquez la taille maximale d'objet pour le téléchargement HTTP/HTTPS (les objets plus grands que cette taille seront bloqués) ou indiquez qu'il n'y a pas de taille maximale pour le téléchargement d'objet via HTTP/HTTPS. • **Taille** maximale de téléchargement FTP : indiquez la taille d'objet maximale pour le téléchargement FTP (les objets plus grands que cette taille seront bloqués) ou indiquez qu'il n'y a pas de taille maximale pour le téléchargement d'objets par FTP.
Type d'objet de blocage	
Archives	Développez cette section pour sélectionner les types de fichiers d'archive à bloquer. Cette liste comprend les types d'archives tels que ARC, BinHex et Stuffit.

Inspectable Archives (Archives pouvant être inspectées)	Développez cette section pour choisir d'**autoriser**, de **bloquer** ou d'**inspecter** des types spécifiques de fichiers d'archive analysables. Les archives pouvant être inspectées sont des fichiers d'archives ou des fichiers compressés que Secure Web Appliance peut gonfler pour inspecter chacun des fichiers qu'il contient afin d'appliquer la politique de blocage des types de fichiers. La liste des archives pouvant être inspectées comprend des types d'archives tels que 7zip, Microsoft CAB, RAR et TAR.
	
	Les points suivants s'appliquent à l'inspection des archives :
	• Seuls les types d'archives marqués **Inspect** (Inspecter) seront gonflés et inspectés.
	• Une seule archive à la fois est inspectée. Les archives pouvant être inspectées simultanément ne peuvent pas être inspectées.
	• Si une archive inspectée contient un type de fichier auquel l'action de blocage est affectée par la politique actuelle, l'archive entière sera bloquée, quels que soient les types de fichiers autorisés qu'elle peut contenir.
	• Une archive inspectée qui contient un type d'archive non pris en charge sera marquée comme « non analysable ». Si elle contient un type d'archive bloqué, elle sera bloquée.
	• Les archives protégées par mot de passe et chiffrées ne sont pas prises en charge et seront marquées comme « non analysables ».
	• Une archive pouvant être inspectée qui est incomplète ou corrompue est marquée comme « non analysable ».
	• La valeur **DVS Engine Object Scanning Limits** (Limites d'analyse des objets du moteur DVS) spécifiées pour les paramètres globaux **Anti-Malware and Reputation** (Programmes malveillants et de réputation) s'applique également à la taille d'une archive pouvant être inspectée; un objet dépassant cette taille est marqué comme « unscannable » (non analysable). Consultez Activation des filtres contre les programmes malveillants et de réputation, à la page 310 pour obtenir des renseignements sur cette limite de taille d'objet.
	• Une archive pouvant être inspectée marquée comme « unscannable » (non analysable) peut être entièrement bloquée ou autorisée.
	• Lorsque les politiques d'accès sont configurées pour bloquer les types MIME personnalisés et que l'inspection des archives est activée :
	  • Si l'appliance télécharge directement un fichier avec le type MIME personnalisé dans l'en-tête content-type, l'accès est bloqué.
	  • Si le même fichier fait partie d'un fichier ZIP/d'archive, l'appliance inspecte l'archive et détermine le type MIME en fonction de sa propre évaluation MIME. Si le type MIME évalué par le moteur de l'appliance ne correspond pas au type MIME personnalisé configuré, le contenu n'est pas bloqué.
	• L'appliance peut inspecter les archives configurées, mais elle est limitée par l'inspection de certaines archives telles que RAR et 7-Zip.
	
	Consultez Paramètres d'inspection des archives, à la page 264 pour obtenir des renseignements sur la configuration de l'inspection des archives.

Document Types (Types de documents)	Développez cette section pour sélectionner les types de documents texte à bloquer. Cette liste comprend les types de documents tels que FrameMaker, Microsoft Office et PDF.
Executable Code (Code exécutable)	Développez cette section pour sélectionner les types de code exécutable à bloquer. La liste comprend Java Applet, UNIX Executable et Windows Executable.
Installers (Programmes d'installation)	Les types de programmes d'installation à bloquer; la liste comprend les ensembles UNIX/LINUX.
Media (Médias)	Types de fichiers multimédias à bloquer. La liste comprend les formats de traitement d'image audio, vidéo et photo (TIFF/PSD).
P2P Metafiles (Métafichiers P2P)	Cette liste comprend les liens BitTorrent Links (`.torrent`).
Web Page Content (Contenu de page Web)	Cette liste comprend les éléments Flash et les images.
Miscellaneous (Divers)	Cette liste comprend les données de calendrier.
Custom MIME Types (Types MIME personnalisés)	Vous pouvez définir des objets/fichiers supplémentaires à bloquer en fonction du type MIME. Entrez un ou plusieurs types MIME dans le champ **Block Custom MIME Types** (Bloquer les types MIME personnalisés), un par ligne.

Étape 4 Cliquez sur **Submit** (Soumettre).

Paramètres d'inspection des archives

Vous pouvez autoriser, bloquer ou inspecter des types spécifiques d'archives pouvant être inspectées pour les politiques d'accès individuelles. Les archives pouvant être inspectées sont des fichiers d'archives ou des fichiers compressés que Secure Web Appliance peut gonfler pour inspecter chacun des fichiers qu'il contient afin d'appliquer la politique de blocage des types de fichiers. Consultez Politiques d'accès : blocage d'objets, à la page 262 pour en savoir plus sur la configuration de l'inspection des archives pour les politiques d'accès individuelles.

Remarque Lors de l'inspection des archives, les objets imbriqués sont écrits sur le disque pour examen. La quantité d'espace disque qui peut être occupée à tout moment pendant l'inspection des fichiers est de 1 Go. Tout fichier d'archive dépassant cette taille maximale d'utilisation du disque sera marqué comme non analysable.

La page Acceptable Use Controls de Secure Web Appliancefournit des paramètres d'archives pouvant être inspectées à l'échelle du système; c'est-à-dire que ces paramètres s'appliquent à l'extraction et à l'inspection des archives lorsque cela est activé dans une politique d'accès.

Étape 1 Choisissez **Security Services** > **Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable).

Étape 2 Cliquez sur le bouton **Edit Archive Settings** (Modifier les paramètres d'archives).

Étape 3 Modifiez les paramètres des archives pouvant être inspectées au besoin.

- **Maximum Encapsulated Archive Extractions** (Nombre maximal d'extractions d'archives encapsulées) : nombre maximal d'archives « encapsulées » à extraire et à inspecter. C'est-à-dire la profondeur maximale pour l'inspection d'une archive contenant d'autres archives pouvant être inspectées. Une archive encapsulée est une archive contenue dans un autre fichier d'archive. Cette valeur peut être comprise entre zéro et cinq; le décompte de profondeur commence à un avec le premier fichier imbriqué.

  L'archive externe est considérée comme le fichier zéro. Si l'archive contient des fichiers imbriqués au-delà de cette valeur imbriquée maximale, l'archive est marquée comme non analysable. Notez que cela aura une incidence sur les performances.

- **Block Uninspectable Archives** (Bloquer les archives non inspectables) : si cette case est cochée, Secure Web Appliance bloquera les archives qu'il n'a pas réussi à exploser et à inspecter.

Étape 4 **Envoyez** et **validez les modifications**.

Bloquer, autoriser ou rediriger les demandes de transactions

Le proxy Web contrôle le trafic Web en fonction des politiques que vous créez pour les groupes de demandes de transaction.

- **Allow (Autoriser).** Le proxy Web permet la connexion sans interruption. Les connexions autorisées n'ont peut-être pas été analysées par le moteur DVS.
- **Block (Bloquer).** Le proxy Web n'autorise pas la connexion et affiche plutôt une page de notification à l'utilisateur final expliquant le motif du blocage.
- **Redirect (Rediriger).** Le proxy Web n'autorise pas la connexion au serveur de destination demandé à l'origine et se connecte plutôt à une autre URL spécifiée; consultez Redirection du trafic dans les politiques d'accès, on page 221.

Note Les actions précédentes sont les actions finales que le proxy Web exécute sur une demande du client. L'action Monitor (Superviser) que vous pouvez configurer pour les politiques d'accès n'est pas une action finale.

En général, différents types de politiques contrôlent le trafic en fonction du protocole de transport.

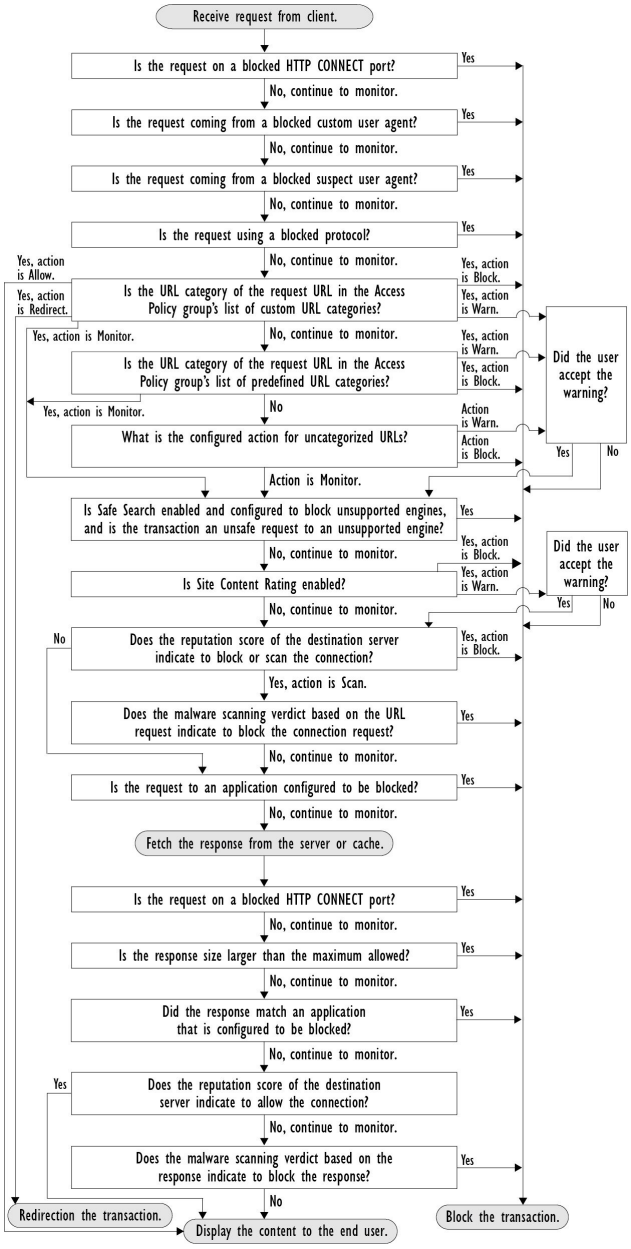
Type de politique	**Protocols (Protocoles)**				**Actions prises en charge**			
	HTTP	HTTPS	FTP	SOCKS	Block (Bloquer)	Allow (Autoriser)	Rediriger	Monitor (Superviser)
Accès	x	x	x		x	x	x	x
SOCKS				x	x	x		
SaaS	x	x						
Déchiffrement	x	x						x
Sécurité des données	x	x	x		x			x

Type de politique	Protocols (Protocoles)				Actions prises en charge			
DLP externe	x	x	x				x	
Analyse des programmes malveillants sortants	x	x	x		x			x
Routage	x	x	x				x	

Note La politique de déchiffrement prévaut sur la politique d'accès.

Le diagramme suivant montre comment le proxy Web détermine l'action à effectuer sur une demande après avoir affecté une politique d'accès particulière à la demande. Le score de réputation Web du serveur de destination est évalué une seule fois, mais le résultat est appliqué à deux étapes différentes dans le flux de décision.

Figure 5: Application des actions de politique d'accès



Applications client

À propos des applications clientes

Les applications clientes (comme un navigateur Web) sont utilisées pour formuler des demandes. Vous pouvez définir l'appartenance aux politiques en fonction des applications clientes, et vous pouvez spécifier des

paramètres de contrôle et dispenser les applications clientes de l'authentification, ce qui est utile pour les applications qui ne peuvent pas demander des informations d'authentification.

Utilisation des applications clientes dans les politiques

Définition de l'appartenance à la politique à l'aide des applications clientes

Étape 1 Choisissez un type de politique dans le menu Web Security Manager.

Étape 2 Cliquez sur un nom de politique dans le tableau des politiques.

Étape 3 Développez la section Advanced (Niveau avancé) et cliquez sur le lien dans le champ Client Applications (Applications clientes).

Étape 4 Définissez une ou plusieurs des applications clientes :

Option	Méthode
Choose a predefined client application (Choisir une application cliente prédéfinie)	Développez les sections Browser (Navigateur) et Other (Autre) et cochez les cases de l'application cliente requise. **Tip** Choisissez uniquement les options Any Version (Toute version) lorsque cela est possible, car cela offre de meilleures performances que d'avoir plusieurs sélections.
Define a custom client application (Définir une application cliente personnalisée)	Entrez une expression régulière appropriée dans le champ Custom Client Applications (Applications clientes personnalisées). Saisissez des expressions régulières supplémentaires sur les nouvelles lignes, le cas échéant. **Tip** Cliquez sur **Exemples de modèles d'applications client** pour obtenir des exemples d'expressions régulières.

Étape 5 (Facultatif) Cliquez sur le bouton d'option Match All Except The Selected **Client Applications** Definitions (Correspondre à toutes les définitions des applications clients hormis celles qui ont été sélectionnées) pour baser l'appartenance à la politique sur toutes les applications clientes, à l'**exception** de celles que vous avez définies.

Étape 6 Cliquez sur **Done** (Terminé).

Définition des paramètres de contrôle des politiques à l'aide des applications clientes

Étape 1 Choisissez un type de politique dans le menu Web Security Manager.

Étape 2 Recherchez le nom de la politique requise dans le tableau des politiques.

Étape 3 Cliquez sur le lien de la cellule dans la colonne Protocols and Client Applications (Protocoles et applications clientes) sur la même ligne.

Étape 4 Choisissez **Define Custom Settings** (Définir des paramètres personnalisés) dans la liste déroulante du volet Edit Protocols and Client Applications Settings (Modifier les protocoles et les paramètres des applications clientes) (si ce n'est pas déjà fait).

Étape 5 Entrez une expression régulière dans le champ Custom Client Applications (Applications clientes personnalisées) qui correspond à l'application cliente que vous souhaitez définir. Saisissez des expressions régulières supplémentaires sur les nouvelles lignes, le cas échéant.

Tip Cliquez sur **Example Client Application Patterns** (Exemple de modèles d'application cliente) pour obtenir des exemples d'expressions régulières.

Étape 6 Envoyez et validez vos modifications.

Dispense d'authentification pour les applications clientes

Procedure

	Command or Action	Purpose
Étape 1	Créez un profil d'identification qui ne nécessite pas d'authentification.	Classification des utilisateurs et logiciels clients, on page 153
Étape 2	Définissez l'appartenance au profil d'identification comme application cliente à dispenser.	Utilisation des applications clientes dans les politiques, on page 268
Étape 3	Placez le profil d'identification au-dessus de tous les autres profils d'identification dans le tableau des politiques qui nécessitent une authentification.	Ordre des politiques, on page 252

Plages de temps et quotas

Vous pouvez appliquer des plages de temps et des quotas de temps et de volumes pour établir des politiques d'accès et de déchiffrement à restreindre quand un utilisateur a un accès, ainsi que sa durée de connexion ou son volume de données maximal (également appelé « quota de bande passante »).

- Plages de temps pour les politiques et contrôles d'utilisation acceptable, on page 269
- Quotas de temps et de volume, on page 270

Plages de temps pour les politiques et contrôles d'utilisation acceptable

Les plages de temps sont des périodes définies pendant lesquelles les politiques et les contrôles d'utilisation acceptable s'appliquent.

Note Vous ne pouvez pas utiliser des plages de temps pour définir les heures auxquelles les utilisateurs doivent s'authentifier. Les exigences d'authentification sont définies dans les profils d'identification, qui ne prennent pas en charge les plages de temps.

- Création d'une plage de temps, on page 270

Création d'une plage de temps

Étape 1 Choisissez **Web Security Manager** > **Define Time Ranges and Quotas** (Web Security Manager > Définir les plages de temps et les quotas).

Étape 2 Cliquez sur **Add Time Range** (Ajouter la plage de temps).

Étape 3 Attribuez un nom à la plage de temps.

Étape 4 Choisissez une option de **Time Zone** (Fuseau horaire) :

- **Use Time Zone Setting From Appliance** (Utiliser les paramètres de fuseau horaire de l'appliance) : utilisez le même fuseau horaire que Secure Web Appliance.
- **Specify Time Zone for this Time Range** (Indiquer le fuseau horaire pour cette plage horaire) : définissez un fuseau horaire différent, soit en tant que décalage GMT ou en tant que région, pays et un fuseau horaire spécifique dans ce pays.

Étape 5 Cochez une ou plusieurs cases **Day of Week** (Jour de la semaine).

Étape 6 Sélectionnez une option **Time of Day** (Heure de la journée) :

- **All Day** (Toute la journée) : utilisez la période complète de 24 heures.
- **From** (Du) et **To** (Au) : définissez une plage d'heures spécifique : saisissez une heure de début et une heure de fin au format HH:MM (format 24 heures).

Tip Chaque plage de temps définit une heure de début et une limite de temps de fin. Par exemple, la saisie de 8:00 à 17:00 correspond à 8:00:00 à 16:59:59, mais pas à 17:00:00. Vous devez définir minuit entre 00:00 pour l'heure de début et 24:00 pour une heure de fin.

Étape 7 Envoyez et validez vos modifications.

Quotas de temps et de volume

Les quotas permettent à un utilisateur de continuer à accéder à une ressource Internet (ou à une classe de ressources Internet) jusqu'à ce qu'il ait épuisé le volume de données ou la limite de temps imposée. AsyncOS applique des quotas définis au trafic HTTP, HTTPS et FTP.

Lorsqu'un utilisateur approche de son quota de temps ou de volume, AsyncOS affiche d'abord un avertissement, puis une page de blocage.

Veuillez noter les points suivants concernant l'utilisation des quotas de temps et de volume :

- Si AsyncOS est déployé en mode transparent et que le proxy HTTPS est désactivé, il n'y a pas d'écoute sur le port 443 et les demandes sont abandonnées. Il s'agit d'un comportement standard. Si AsyncOS est déployé en mode explicite, vous pouvez définir des quotas dans vos politiques d'accès.

  Lorsque le proxy HTTPS est activé, les actions possibles sur une demande sont la transmission, le déchiffrement, la suppression ou la supervision. Dans l'ensemble, les quotas dans les politiques de déchiffrement ne s'appliquent qu'aux catégories d'intercommunication.

  Avec l'interconnexion, vous aurez également la possibilité de définir des quotas pour le trafic du tunnel. Avec déchiffrement, cette option n'est pas disponible, car les quotas configurés dans la politique d'accès seront appliqués au trafic déchiffré.

- Si le filtrage d'URL est désactivé ou si sa clé de fonctionnalité n'est pas disponible, AsyncOS ne peut pas identifier la catégorie d'une URL et la page **Access Policy** > **URL Filtering** (Politique d'accès > Filtrage d'URL) est désactivée. Par conséquent, la clé de fonctionnalité doit être présente et les politiques d'utilisation acceptable activées pour pouvoir configurer les quotas.
- De nombreux sites Web comme Facebook et Gmail sont mis à jour automatiquement à des intervalles réguliers. Si un site Web de ce type est laissé ouvert dans une fenêtre ou un onglet de navigateur inutilisé, il continuera de consommer le quota de temps et de volume de l'utilisateur.
- Lorsque vous redémarrez le proxy et que le mode haute performance est :
  - **Activé** : les quotas de temps et de volume ne sont pas réinitialisés. Les quotas sont automatiquement réinitialisés une fois dans la fenêtre de 24 heures en fonction de l'heure configurée.
  - **Désactivé** : les quotas de temps et de volume sont réinitialisés. L'incidence de la réinitialisation ne perdure que pour la fenêtre actuelle de 24 heures, car les quotas sont automatiquement réinitialisés une fois dans toutes les 24 heures. Le proxy peut redémarrer en raison de modifications de configuration ou d'un plantage du processus de proxy.
- Vos pages EUN (d'avertissement et de blocage) ne peuvent pas être affichées pour HTTPS même lorsque l'option decrypt-for-EUN est activée.

Note Le quota le plus restrictif s'appliquera toujours lorsque plusieurs quotas s'appliquent à un utilisateur donné.

- Calculs du quota de volume, on page 271
- Calculs des quotas de temps, on page 271
- Définition des quotas de temps, de volume et de bande passante, on page 272

Calculs du quota de volume

Le calcul des quotas de volume se fait comme suit :

- Trafic HTTP et HTTPS déchiffré : le corps de la demande et de la réponse HTTP sont pris en compte dans les limites de quota. Les en-têtes de demande et les en-têtes de réponse ne seront pas pris en compte dans le calcul des limites.
- Trafic tunnelisé (y compris HTTPS tunnelisé) : AsyncOS transfère simplement le trafic tunnelisé du client au serveur, et inversement. L'intégralité du volume de données du trafic tunnelisé est pris en compte dans les limites de quota.
- FTP : le trafic de connexion de contrôle n'est pas pris en compte. La taille du fichier chargé et téléchargé est prise en compte dans les limites de quota.

Note Seul le trafic côté client est pris en compte dans les limites de quota. Le contenu en cache est également pris en compte dans la limite, car le trafic côté client est généré même lorsqu'une réponse est fournie à partir du cache.

Calculs des quotas de temps

Le calcul des quotas de temps est le suivant :

- Trafic HTTP et HTTPS déchiffré : la durée de chaque connexion à la même catégorie d'URL, de sa formation à la déconnexion, plus une minute, est prise en compte dans la limite des quotas de temps. Si

plusieurs demandes sont adressées à la même catégorie d'URL à moins d'une minute d'intervalle, elles sont comptées comme une session continue et la minute est ajoutée uniquement à la fin de cette session (c'est-à-dire après au moins une minute de « silence »).

- Trafic de tunnel (y compris HTTPS en tunnel) : La durée réelle du tunnel, de sa formation à la déconnexion, est prise en compte dans les limites des quotas. Le calcul ci-dessus pour les demandes multiples s'applique également au trafic en tunnel.
- FTP : La durée réelle de la session de contrôle FTP, de sa création à la déconnexion, est prise en compte dans les limites des quotas. Le calcul ci-dessus pour les demandes multiples s'applique également au trafic FTP.

Définition des quotas de temps, de volume et de bande passante

Before you begin

- Accédez à **Security Services** > **Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable) pour activer Acceptable Use Controls (Contrôles d'utilisation acceptable).
- Définissez une plage de temps, sauf si vous souhaitez que le quota s'applique comme limite quotidienne.

Étape 1 Accédez à **Web Security Manager > Define Time Ranges and Quotas** (Web Security Manager > Définir des plages de temps et des quotas).

Étape 2 Cliquez sur **Add Quota** (Ajouter un quota).

Étape 3 Entrez un **nom de quota** unique dans le champ.

Étape 4 Pour réinitialiser le quota d'heure et de volume tous les jours, sélectionnez **Reset Time and Volume quota daily at** (Réinitialiser ce quota quotidiennement à/Réinitialiser le quota de temps et de volume quotidiennement à) et entrez une heure au format 12 heures dans le champ, puis choisissez **AM** ou **PM** dans le menu. Vous pouvez également sélectionner **Select a predefined time range profile** (Sélectionner un profil de plage de temps prédéfini).

Note L'utilisation de l'option de réinitialisation du quota ne réinitialise pas la valeur configurée du quota de bande passante.

Étape 5 Pour définir un quota de temps, cochez la case **Time Quota** (Quota de temps) et choisissez le nombre d'heures dans le menu **hrs** et le nombre de minutes dans le menu **mins**, de zéro (toujours bloqué) à 23 heures et 59 minutes.

Étape 6 Pour définir un quota de volume, saisissez une valeur dans le champ et sélectionnez **KB** (Ko, kilooctets), MB (Mo, mégaoctets) ou **GB** (Go, gigaoctets) dans le menu.

Étape 7 Pour définir un quota de bande passante, saisissez une valeur dans le champ et choisissez **Kbit/s** (kilobits par seconde) ou **Mbit/s** (mégabits par seconde) dans le menu.

- Le quota de bande passante peut être configuré uniquement dans la politique d'accès. Cependant, vous ne pouvez pas configurer les deux, le quota de bande passante URL et le quota d'activité Web globale pour une même politique d'accès.
- Le quota de bande passante ne peut pas être configuré si la limite de bande passante globale ou la limite de bande passante AVC est activée, et inversement.
- Le contenu en cache est également pris en compte pour le quota de bande passante.
- Nous vous déconseillons d'ajouter un quota de bande passante à un profil de quota de temps ou de volume existant qui est mappé à la politique de déchiffrement ou à la politique CDS.

Bien que vous puissiez modifier le profil de quota, vous ne pouvez pas configurer le quota de bande passante sur une politique de déchiffrement et de CDS.

Note Supprimez tous les profils de quota dont le quota de bande passante a été configuré avant la mise à niveau vers AsyncOS version 14.5.

Étape 8 Cliquez sur **Submit** (Envoyer), puis sur **Commit Changes** (Valider les modifications) pour appliquer vos modifications. Vous pouvez également cliquer sur **Cancel** (Annuler) pour abandonner vos modifications.

What to do next

(Facultatif) Accédez à **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final) pour configurer les notifications de l'utilisateur final concernant les quotas.

Contrôle d'accès par catégorie d'URL

Vous pouvez définir et traiter les demandes Web en fonction de la catégorie de sites Web sur laquelle elles portent. Secure Web Appliance est fourni avec de nombreuses catégories d'URL prédéfinies, comme les courriels basés sur le Web et autres.

Les catégories prédéfinies, et les sites Web qui y sont associés, sont définis dans les bases de données de filtrage qui résident sur le Secure Web Appliance. Ces bases de données sont automatiquement mises à jour par Cisco. Vous pouvez également créer des catégories d'URL personnalisées pour les noms d'hôte et les adresses IP que vous spécifiez.

Les catégories d'URL peuvent être utilisées par toutes les politiques, à l'exception des politiques d'identification des demandes. Elles peuvent également être utilisées par les politiques d'accès, de gestion HTTPS chiffré et de sécurité des données pour appliquer des actions aux demandes.

Voir Création et modification de catégories d'URL personnalisées, on page 211 pour plus d'informations sur la création de catégories d'URL personnalisées.

Utilisation de catégories d'URL pour identifier les demandes Web

Before you begin

- Activez Acceptable Use Control, consultez Configuration du moteur de filtrage d'URL , on page 194.
- (Facultatif) Créez des catégories d'URL personnalisées, consultez Création et modification de catégories d'URL personnalisées, on page 211.

Étape 1 Choisissez un type de politique (sauf SaaS) dans le menu Web Security Manager.

Étape 2 Cliquez sur un nom de politique dans le tableau des politiques (ou ajoutez une nouvelle politique).

Étape 3 Développez la section **Advanced** (Niveau avancé) et cliquez sur le lien dans le champ URL Categories (Catégories d'URL).

Étape 4 Cliquez sur les cellules de colonne Add (Ajouter) correspondant aux catégories d'URL selon lesquelles vous souhaitez identifier les demandes Web. Effectuez cette opération pour les listes de catégories d'URL personnalisées et de catégories d'URL prédéfinies, le cas échéant.

Étape 5 Cliquez sur **Done** (Terminé).

Étape 6 Envoyez et validez vos modifications.

Utilisation de catégories d'URL pour traiter une demande Web

Before you begin

- Activez Acceptable Use Control, consultez Configuration du moteur de filtrage d'URL , on page 194.
- (Facultatif) Créez des catégories d'URL personnalisées, consultez Création et modification de catégories d'URL personnalisées, on page 211.

Note Si vous avez utilisé des catégories d'URL comme critères dans une politique, ces catégories seules sont disponibles pour spécifier des actions au sein de la même politique. Certaines des options décrites ci-dessous peuvent être différentes ou ne pas être disponibles pour cette raison.

Étape 1 Choisissez entre **Access Policies** (Politiques d'accès), **Cisco Data Security Policies** (Politiques de sécurité des données Cisco) ou **Encrypted HTTPS Management** (Gestion HTTPS chiffrée) dans le menu Web Security Manager.

Étape 2 Recherchez le nom de la politique requise dans le tableau des politiques.

Étape 3 Cliquez sur le lien de la cellule dans la colonne URL Filtering (Filtrage d'URL) sur la même ligne.

Étape 4 (Facultatif) Ajoutez des catégories d'URL personnalisées :

a) Cliquez sur **Select Custom Categories** (Sélectionner des catégories personnalisées).

b) Choisissez les catégories d'URL personnalisées à inclure dans cette politique et cliquez sur **Apply** (Appliquer).

Choisissez les catégories d'URL personnalisées auxquelles le moteur de filtrage d'URL doit comparer la demande du client. Le moteur de filtrage d'URL compare les demandes des clients aux catégories d'URL personnalisées incluses et ignore les catégories d'URL personnalisées exclues. Le moteur de filtrage d'URL compare l'URL dans une demande d'un client aux catégories d'URL personnalisées incluses avant les catégories d'URL prédéfinies.

Les catégories d'URL personnalisées incluses dans la politique apparaissent dans la section Custom URL Category Filtering (Filtrage de catégories d'URL personnalisées).

Étape 5 Choisissez une action pour chaque catégorie d'URL personnalisée et prédéfinie.

Note Les actions disponibles varient selon les catégories personnalisées et prédéfinies, et selon les types de politiques.

Étape 6 Dans la section Uncategorized URLs (URL non classées), choisissez l'action à entreprendre pour les demandes des clients adressées aux sites Web qui n'entrent pas dans une catégorie d'URL prédéfinie ou personnalisée.

Étape 7 Envoyez et validez vos modifications.

Utilisateurs à distance

- À propos des utilisateurs à distance, on page 275

À propos des utilisateurs à distance

Cisco AnyConnect Secure Mobility étend le périmètre du réseau aux terminaux distants, ce qui permet l'intégration des services de filtrage Web offerts par Secure Web Appliance.

Les utilisateurs mobiles et distants utilisent le client Cisco AnyConnect Secure VPN (réseau privé virtuel) pour établir des sessions VPN avec Adaptive Security Appliance (ASA). L'ASA envoie le trafic Web à Secure Web Appliance avec des informations identifiant l'utilisateur par adresse IP et par nom d'utilisateur. Secure Web Appliance analyse le trafic, applique les politiques d'utilisation acceptable et protège l'utilisateur contre les menaces à la sécurité. L'appliance de sécurité renvoie tout le trafic jugé sûr et acceptable à l'utilisateur.

Lorsque Secure Mobility est activé, vous pouvez configurer les identités et les politiques à appliquer aux utilisateurs en fonction de leur emplacement :

- **Utilisateurs à distance.** Ces utilisateurs sont connectés au réseau à partir d'un emplacement distant à l'aide du VPN. Secure Web Appliance identifie automatiquement les utilisateurs à distance lorsque Cisco ASA et le client Cisco AnyConnect sont utilisés pour l'accès VPN. Sinon, l'administrateur Secure Web Appliance doit indiquer les utilisateurs à distance en configurant une plage d'adresses IP.
- **Utilisateurs locaux.** Ces utilisateurs sont connectés au réseau physiquement ou sans fil.

Quand Secure Web Appliance est intégré à Cisco ASA, vous pouvez le configurer pour identifier les utilisateurs par un nom d'utilisateur authentifié de manière transparente afin de permettre la connexion unique pour les utilisateurs à distance.

Comment configurer l'identification des utilisateurs à distance

Tâche	Informations complémentaires
1. Configurez l'identification des utilisateurs à distance.	Configuration de l'identification des utilisateurs à distance, on page 276
2. Créez une identité pour les utilisateurs à distance.	Classification des utilisateurs et logiciels clients, on page 153 1. Dans la section « Define Member by User Location » (Définir les membres par emplacement utilisateur), sélectionnez Remote Users Only (Utilisateurs à distance uniquement). 2. Dans la section « Define Member by Authentication » (Définir les membres par l'authentification), sélectionnez « Identify Users Clearly using Cisco ASA integration » (Identifier les utilisateurs de manière transparente par l'intégration Cisco ASA).
3. Créez une politique pour les utilisateurs à distance.	Création d'une politique , on page 253

Configuration de l'identification des utilisateurs à distance

Étape 1 Services de sécurité > AnyConnect Secure Mobility, puis cliquez sur **Enable** (Activer).

Étape 2 Lisez les conditions du contrat de licence d'AnyConnect Secure Mobility, puis cliquez sur **Accept** (Accepter).

Étape 3 Configurez l'identification des utilisateurs à distance.

Option	Description	Étapes supplémentaires
IP Address (Adresse IP)	Indiquez une plage d'adresses IP que l'appliance doit considérer comme attribuées aux périphériques distants.	**a.** Entrez une plage d'adresses IP dans le champ IP Range (Plage d'adresses IP). **b.** Passez à l'étape 4.
Cisco ASA Integration (Intégration Cisco ASA)	Indiquez un ou plusieurs systèmes Cisco ASA avec lesquels Secure Web Appliance communique. Le système Cisco ASA gère un mappage entre l'adresse IP et l'utilisateur et communique cette information à Secure Web Appliance. Lorsque le proxy Web reçoit une transaction, il obtient l'adresse IP et détermine l'utilisateur en vérifiant le mappage entre l'adresse IP et l'utilisateur. Lorsque les utilisateurs sont déterminés par l'intégration avec un système Cisco ASA, vous pouvez activer la connexion unique pour les utilisateurs à distance.	**a.** Saisissez le nom d'hôte ou l'adresse IP du système Cisco ASA. **b.** Saisissez le numéro de port utilisé pour accéder au système ASA. Le numéro de port par défaut du système Cisco ASA est 11999. **c.** Si plusieurs système Cisco ASA sont configurés dans une grappe, cliquez sur **Add Line** (Ajouter une ligne) et configurez chaque système ASA de la grappe. **Note** Si deux systèmes Cisco ASA sont configurés pour la haute disponibilité, saisissez un seul nom d'hôte ou une seule adresse IP pour le système Cisco ASA *actif*. **d.** Saisissez la phrase secrète d'accès pour Cisco ASA. **Note** La phrase secrète que vous entrez ici doit correspondre à la phrase secrète d'accès configurée pour le système Cisco ASA indiqué. **e.** Facultatif, cliquez sur **Start Test** (Commencer le test) pour vérifier que Secure Web Appliance peut se connecter au système Cisco ASA configuré.

Étape 4 Envoyez et validez les modifications.

Note Activez AnyConnect Security Mobility (**Security Services** > **AnyConnect Security Mobility**) (AnyConnect Security Mobility > Services de sécurité > AnyConnect Security Mobility) pour rendre l'option Define Members by User Location (Définir les membres par emplacement utilisateur) disponible sur Secure Web Appliance. Par défaut, cette option est disponible sur l'appliance Cisco de gestion de la sécurité de contenu [**Web** > **Configuration Master** > **Identification Profiles** (Web > Fichier de configuration principal > Profils d'identification)]. Lorsque vous utilisez l'option Define Member by User Location (Définir les membres par emplacement utilisateur) pour configurer un profil d'identification dans l'appliance de gestion de la sécurité et publiez cette configuration sur Secure Web Appliance, où AnyConnect Security Mobility n'est pas activé, le profil d'identification est désactivé.

Affichage de l'état et des statistiques de l'utilisateur distant pour les ASA

Utilisez cette commande pour afficher les informations relatives à Secure Mobility quand Secure Web Appliance est intégré à un ASA.

Commande	Description
`musstatus`	Cette commande affiche les informations suivantes : • L'état de la connexion Secure Web Appliance avec chaque ASA. • La durée de la connexion Secure Web Appliance avec chaque ASA en minutes. • Le nombre de clients distants de chaque ASA. • Le nombre de clients distants desservis, qui est défini comme le nombre de clients distants qui ont transmis du trafic par l'intermédiaire de Secure Web Appliance. • Le nombre total de clients distants.

Résolution de problèmes de politiques

- Politique d'accès non configurable pour HTTPS, on page 651
- Certains fichiers Microsoft Office ne sont pas bloqués, on page 637
- Le blocage des types d'objets exécutables DOS bloque les mises à jour pour Windows OneCare, on page 637
- Disparition du profil d'identification de la politique, on page 652
- La politique n'est jamais appliquée, on page 652
- Les demandes HTTPS et FTP via HTTP correspondent uniquement aux politiques d'accès qui ne nécessitent pas d'authentification, on page 652
- Politique globale de correspondances des utilisateurs pour les demandes HTTPS et FTP via HTTP, on page 653
- Politique d'accès incorrecte attribuée à l'utilisateur , on page 653

- Outil de résolution de problèmes liés aux politiques : Suivi des politiques, on page 653

CHAPITRE 11

Créer des politiques de déchiffrement pour contrôler le trafic HTTPS

Cette rubrique contient les sections suivantes :

Survol de la création de politiques de déchiffrement pour contrôler le trafic HTTPS

Les politiques de déchiffrement définissent le traitement du trafic HTTPS au sein du proxy Web :

- Quand déchiffrer le trafic HTTPS.
- Comment gérer les demandes qui utilisent des certificats de sécurité non valides ou révoqués

Vous pouvez créer des politiques de déchiffrement pour gérer le trafic HTTPS des manières suivantes :

- Transmettez le trafic chiffré
- Déchiffrez le trafic et appliquer les politiques d'accès basées sur le contenu définies pour le trafic HTTP. Cela rend également l'analyse des programmes malveillants possible

  .
- Abandonnez la connexion HTTPS
- Supervisez la demande (n'effectuez aucune action finale) pendant que le proxy Web continue d'évaluer la demande par rapport aux politiques qui peuvent mener à une action finale d'abandon, de transmission ou de déchiffrement.

Caution **Manipulez les informations nominatives avec prudence :** si vous choisissez de déchiffrer la session HTTPS d'un utilisateur final, les journaux d'accès et les rapports Secure Web Appliance peuvent contenir des renseignements nominatifs. L'administrateur peut configurer la quantité de texte d'URI stockée dans les journaux à l'aide de la commande de l'interface de ligne de commande `advancedproxyconfig` et de la sous-commande `HTTPS`. Vous pouvez consigner l'URI entier ou une forme partielle de l'URI en supprimant la partie requête. Cependant, même lorsque vous choisissez de supprimer la requête de l'URI, des renseignements nominatifs peuvent toujours être conservés.

Gestion du trafic HTTPS à l'aide de politiques de déchiffrement – Présentation des tâches

Étape	Liste des tâches pour la gestion du trafic HTTPS par le biais de politiques de déchiffrement	Liens vers des rubriques et des procédures connexes
1	Activation du proxy HTTPS	Activation du proxy HTTPS, on page 283
2	Charger ou générer un certificat et une clé	• Chargement d'un certificat racine et d'une clé, on page 289 • Génération d'un certificat et d'une clé pour le proxy HTTPS, on page 290
3	Configuration des options de déchiffrement	Configuration des options de déchiffrement, on page 286
5	(Facultatif) Configurer la gestion des certificats non valides	Configuration du traitement des certificats non valides, on page 291
6	(Facultatif) Activation de la vérification de l'état de révocation en temps réel	Activation de la vérification de l'état de révocation en temps réel, on page 292
7	(Facultatif) Gérer les certificats approuvés et les certificats bloqués	Certificats racine approuvés, on page 293

Gestion du trafic HTTPS à l'aide de politiques de déchiffrement – Bonnes pratiques

Créez moins de groupes de politiques de déchiffrement plus généraux qui s'appliquent à tous les utilisateurs ou des groupes d'utilisateurs moins nombreux et plus importants sur le réseau. Ensuite, si vous devez appliquer un contrôle plus granulaire au trafic HTTPS déchiffré, utilisez des groupes de politiques d'accès plus spécifiques.

Politiques de déchiffrement

L'appliance peut effectuer l'une des actions suivantes sur une demande de connexion HTTPS :

Option	Description
Monitor (Superviser)	La supervision est une action intermédiaire qui indique que le proxy Web doit continuer à évaluer la transaction par rapport aux autres paramètres de contrôle pour déterminer l'action finale à appliquer.
Drop (abandonner)	L'appliance abandonne la connexion et ne transmet pas la demande de connexion au serveur. L'appliance n'informe pas l'utilisateur qu'il a abandonné la connexion.
Pass through (Intercommunication)	L'appliance traverse la connexion entre le client et le serveur sans inspecter le contenu du trafic. Cependant, avec une politique de transmission standard, Secure Web Appliance vérifie la validité du serveur demandé en déclenchant une liaison HTTPS avec le serveur. Cette vérification de validité inclut la validation du certificat du serveur. En cas d'échec de la vérification du serveur, la transaction est bloquée. Vous pouvez ignorer les contrôles de validation pour des sites spécifiques en configurant des politiques qui intègrent des catégories personnalisées incluant ces sites, indiquant ainsi que ces sites sont fiables : ces sites sont transmis sans contrôles de validité. Faites attention lors de la configuration de politiques qui permettent d'ignorer les contrôles de validité.
Decrypt Déchiffrer	L'appliance autorise la connexion, mais inspecte le contenu du trafic. Il déchiffre le trafic et applique des politiques d'accès au trafic déchiffré comme s'il s'agissait d'une connexion HTTP en texte brut. En déchiffrant la connexion et en appliquant des politiques d'accès, vous pouvez analyser le trafic à la recherche de programmes malveillants.

Toutes les actions, à l'exception de la fonction Superviser, sont des « actions finales » que le proxy Web applique à une transaction. Une action finale est une action qui amène le proxy Web à interrompre l'évaluation de la transaction par rapport à d'autres paramètres de contrôle. Par exemple, si une politique de déchiffrement est configurée pour surveiller les certificats de serveur non valides, le proxy Web ne prend pas de décision finale sur la façon de gérer la transaction HTTPS si le serveur contient un certificat non valide. Si une politique de déchiffrement est configurée pour bloquer les serveurs présentant un score de réputation Web faible, toute demande adressée à un serveur possédant un score de réputation faible est abandonnée sans que les actions de la catégorie d'URL soient prises en compte.

Le diagramme suivant montre comment le proxy Web évalue une demande d'un client par rapport aux groupes de la politique de déchiffrement. Contrôle du trafic HTTPS affiche l'ordre utilisé par le proxy Web lors de l'évaluation des paramètres de contrôle pour les politiques de déchiffrement. Figure 5: Application des actions de politique d'accès, on page 267 indique l'ordre utilisé par le proxy Web lors de l'évaluation des paramètres de contrôle pour les politiques d'accès.

Figure 6: Application des actions de la politique de déchiffrement

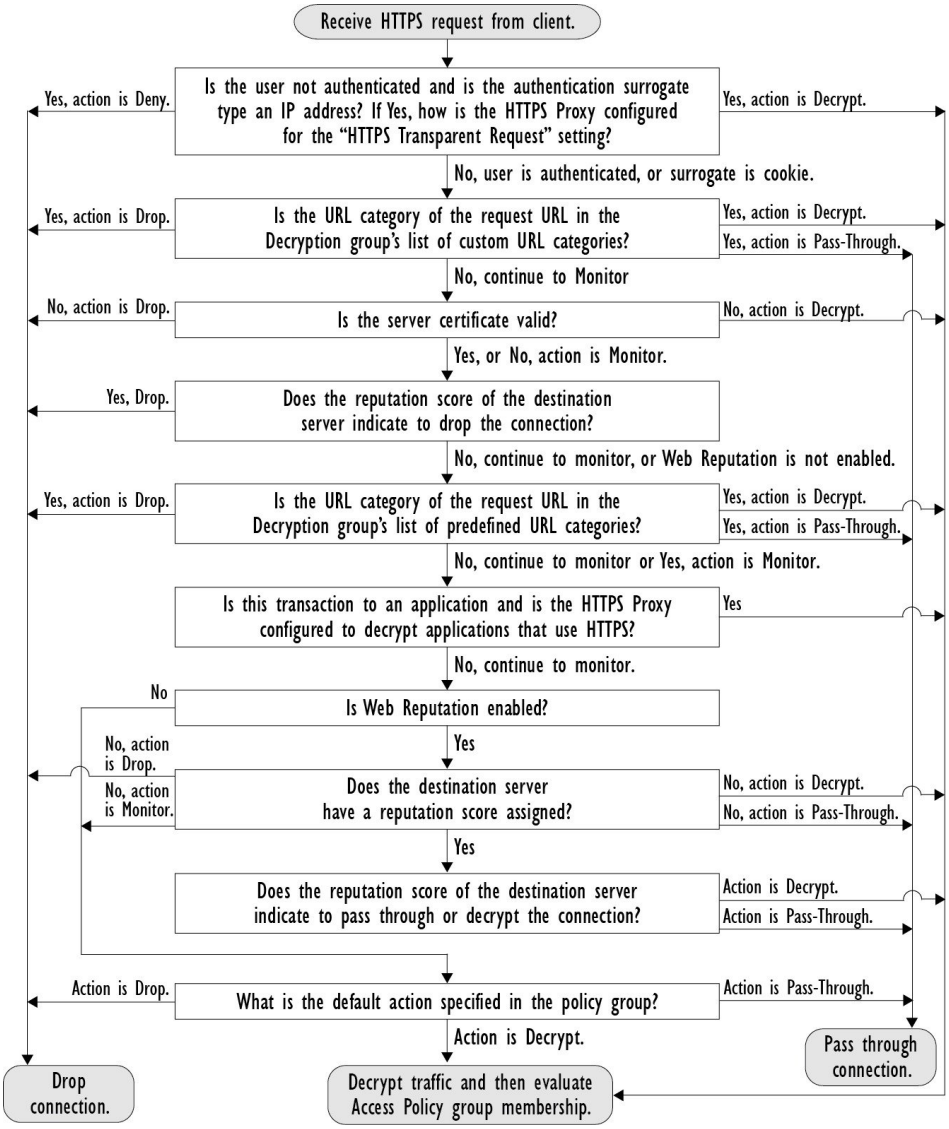
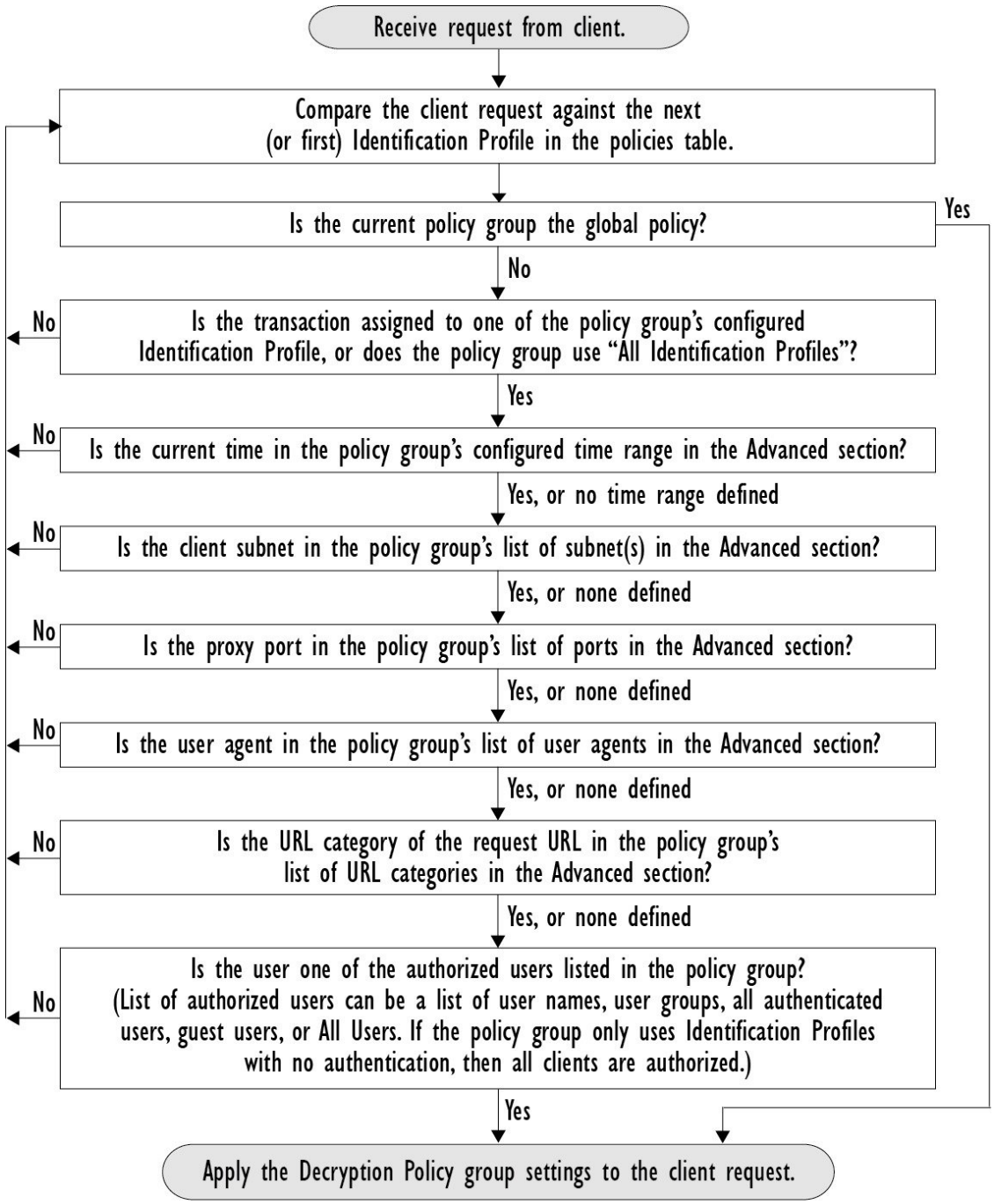


Figure 7: Flux de transaction des groupes de politiques pour les politiques de déchiffrement



Activation du proxy HTTPS

Pour surveiller et déchiffrer le trafic HTTPS, vous devez activer le proxy HTTPS. Lorsque vous activez le proxy HTTPS, vous devez configurer ce que l'appliance utilise comme certificat racine lorsqu'elle envoie des certificats de serveur autosignés aux applications clientes sur le réseau. Vous pouvez télécharger un

certificat racine et une clé dont votre organisation dispose déjà, ou vous pouvez configurer l'appliance de sorte qu'elle génère un certificat et une clé avec les informations que vous saisissez.

Une fois le proxy HTTPS activé, toutes les décisions de politique HTTPS sont prises en charge par les politiques de déchiffrement. Vous pouvez aussi configurer dans cette page ce que l'appliance fait du trafic HTTPS lorsque le certificat du serveur n'est pas valide.

Before you begin

Lorsque le proxy HTTPS est activé, les règles spécifiques à HTTPS dans les politiques d'accès sont désactivées et le proxy Web traite le trafic HTTPS déchiffré à l'aide des règles pour HTTP.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS), cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Le contrat de licence du proxy HTTPS s'affiche.

Étape 2 Lisez les conditions du contrat de licence du proxy HTTPS et cliquez sur **Accept** (Accepter).

Étape 3 Vérifiez que le champ Enable HTTPS Proxy (Activer le proxy HTTPS) est activé.

Étape 4 Dans le champ **HTTPS Ports to Proxy** (Ports HTTPS vers le proxy), saisissez les ports que l'appliance doit vérifier pour le trafic HTTPS. Le port par défaut est 443.

Note Secure Web Appliance peut utiliser un maximum de 30 ports comme proxy : 3 ports sont toujours réservés pour le proxy FTP et 27 ports peuvent être configurés comme proxy HTTP et HTTPS.

Étape 5 Chargez ou générez un certificat racine/de signature à utiliser pour le déchiffrement.

Note Si l'appliance a à la fois un certificat et une paire de clés téléchargés et un certificat et une paire de clés générés, elle utilise uniquement le certificat et la paire de clés actuellement sélectionnés dans la section Root Certificate for Signing (Certificat racine pour signature).

Étape 6 Dans la section HTTPS transparent Request (Demande HTTPS transparente), sélectionnez l'une des options suivantes :

- Decrypt the HTTPS request and redirect for authentication (Déchiffrer la demande HTTPS et rediriger pour authentification)
- Deny the HTTPS request (Refuser la demande HTTPS)

Ce paramètre s'applique uniquement aux transactions qui utilisent l'adresse IP comme substitution d'authentification et lorsque l'utilisateur n'a pas encore été authentifié.

Note Ce champ ne s'affiche que lorsque l'appliance est déployée en mode transparent.

Étape 7 **Note** Le déchiffrement peut faire échouer certaines applications, sauf si le certificat racine de signature est installé sur le client. Pour en savoir plus sur le certificat racine de l'appliance, consultez Gestion de la validation et du déchiffrement des certificats pour HTTPS, on page 288.

Étape 8 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

• Gestion de la validation et du déchiffrement des certificats pour HTTPS, on page 288

Contrôle du trafic HTTPS

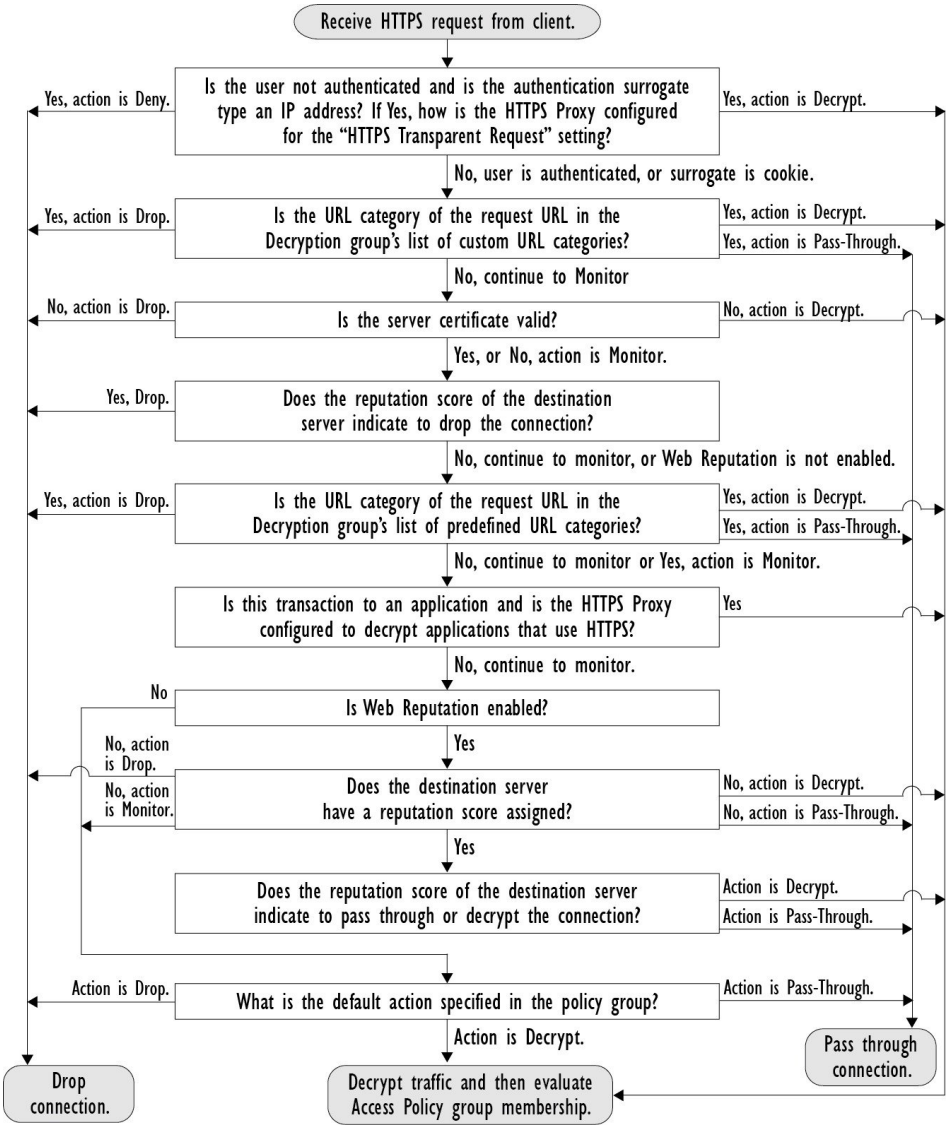
Après que Secure Web Appliance a affecté une demande de connexion HTTPS à un groupe de politiques de déchiffrement, la demande de connexion hérite des paramètres de contrôle de ce groupe de politiques. Les paramètres de contrôle du groupe de politiques de déchiffrement déterminent si l'appliance déchiffre, abandonne ou transmet la connexion :

Option	Description
URL Categories (Catégories d'URL)	Vous pouvez configurer l'action à entreprendre sur les demandes HTTPS pour chaque catégorie d'URL prédéfinie et personnalisée. Cliquez sur le lien sous la colonne URL Filtering (Filtrage d'URL) pour le groupe de politiques que vous souhaitez configurer. **Note** Si vous souhaitez *bloquer* (avec notification de l'utilisateur final) une catégorie d'URL particulière pour les demandes HTTPS au lieu de l'abandonner (sans notification de l'utilisateur final), choisissez de déchiffrer cette catégorie d'URL dans le groupe de politiques de déchiffrement, puis choisissez de bloquer la même URL dans le groupe de politiques d'accès.
Web Reputation (Réputation Web)	Vous pouvez configurer l'action à entreprendre sur les demandes HTTPS en fonction du score de réputation Web du serveur demandé. Cliquez sur le lien sous la colonne Web Reputation (Réputation Web) pour le groupe de politiques que vous souhaitez configurer.
Default Action (Action par défaut)	Vous pouvez configurer l'action que l'appliance doit effectuer quand aucun des autres paramètres ne s'applique. Cliquez sur le lien sous la colonne Default Action (Action par défaut) pour le groupe de politiques que vous souhaitez configurer. **Note** L'action configurée par défaut n'affecte la transaction que si aucune décision n'est prise en fonction de la catégorie d'URL ou du score de réputation Web. Si le filtrage de réputation Web est désactivé, l'action par défaut s'applique à toutes les transactions qui correspondent à une action Monitor (Superviser) dans une catégorie d'URL. Si le filtrage de réputation Web est activé, l'action par défaut est utilisée uniquement si l'action Monitor (Superviser) est sélectionnée pour les sites sans score de réputation.

Pour contourner le trafic chiffré ayant un bon score de réputation Web, assurez-vous de désactiver l'option **Decrypt for Application Detection** (Déchiffrer pour la détection des applications) dans la section **Decryption Options** (Options de déchiffrement) de la page HTTPS Proxy Settings (Paramètres du proxy HTTPS).

Le diagramme suivant montre comment l'appliance détermine l'action à exécuter sur une demande HTTPS après avoir affecté une politique de déchiffrement particulière à la demande. Le score de réputation Web du serveur de destination est évalué une seule fois, mais le résultat est appliqué à deux étapes différentes dans le flux de décision. Par exemple, l'action Drop (Abandonner) du score de réputation Web remplace toute action spécifiée pour les catégories d'URL prédéfinies.

Figure 8: Application des actions de la politique de déchiffrement



Configuration des options de déchiffrement

Before you begin

Vérifiez que le proxy HTTPS est activé, comme décrit dans Activation du proxy HTTPS, on page 283.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Activez les options de déchiffrement.

Option de déchiffrement	Description
Decrypt for Authentication (Déchiffrer pour authentification)	Pour les utilisateurs qui n'ont pas été authentifiés avant cette transaction HTTPS, autorisez le déchiffrement pour l'authentification.
Decrypt for End-User Notification (Déchiffrer pour notification à l'utilisateur final)	Autorisez le déchiffrement pour qu'AsyncOS puisse afficher la notification de l'utilisateur final. **Note** Si le certificat est non valide et que les certificats non valides sont définis pour être abandonnés, lors de l'exécution d'une trace de politique, la première action enregistrée pour la transaction est « decrypt » (déchiffrer).
Decrypt for End-User Acknowledgment (Déchiffrer pour l'accusé de réception de l'utilisateur final)	Pour les utilisateurs qui n'ont pas accusé réception du proxy Web avant cette transaction HTTPS, autorisez le déchiffrement pour qu'AsyncOS puisse afficher l'accusé de réception de l'utilisateur final.
Decrypt for Application Detection (Déchiffrer pour la détection d'applications)	Améliore la capacité d'AsyncOS à détecter les applications HTTPS.

Authentification et connexions HTTPS

L'authentification au niveau de la couche de connexion HTTPS est disponible pour les types de demandes suivants :

Option	Description
Explicit requests (Demandes explicites)	• authentification sécurisée du client désactivée ou • authentification sécurisée du client activée et substitution basée sur IP
Transparent requests (Demandes transparentes)	• Substitution basée sur IP, déchiffrement pour l'authentification activé ou • substitution basée sur IP, client authentifié précédemment à l'aide d'une demande HTTP

Certificats racines

Le proxy HTTPS utilise les certificats racine et les fichiers de clé privée que vous chargez sur l'appliance pour déchiffrer le trafic. Le certificat racine et les fichiers de clé privée que vous chargez sur l'appliance doivent être au format PEM; le format DER n'est pas pris en charge.

Vous pouvez saisir les informations de certificat racine comme suit :

- **Generate (Générer).** Vous pouvez saisir des informations de base sur l'organisation, puis cliquer sur un bouton pour que l'appliance génère le reste du certificat et une clé privée.

- **Upload (Charger).** Vous pouvez charger un fichier de certificat et le fichier de clé privée correspondant créé hors de l'appliance.

Note Vous pouvez également charger un certificat intermédiaire signé par une autorité de certification racine. Lorsque le proxy Web imite le certificat du serveur, il envoie le certificat chargé avec le certificat imité à l'application client. De cette façon, tant que le certificat intermédiaire est signé par une autorité de certification racine approuvée par l'application cliente, l'application fera également confiance au certificat de serveur imité. Consultez À propos des certificats et des clés, on page 609 pour obtenir de plus amples renseignements.

Vous pouvez choisir comment gérer les certificats racine émis par Secure Web Appliance :

- **Inform users to accept the root certificate (Informer les utilisateurs d'accepter le certificat racine).** Vous pouvez informer les utilisateurs de votre organisation des nouvelles politiques de l'entreprise et leur dire d'accepter le certificat racine fourni par l'entreprise en tant que source de confiance.
- **Add the root certificate to client machines (Ajouter le certificat racine sur les machines clientes).** Vous pouvez ajouter le certificat racine sur toutes les machines clientes du réseau en tant qu'autorité de certification racine approuvée. De cette façon, les applications client acceptent automatiquement les transactions avec le certificat racine.

Étape 1 Security Services > HTTPS Proxy (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cliquez sur le lien Download Certificate (Télécharger le certificat) correspondant au certificat généré ou chargé.

Note Pour réduire la possibilité que les machines clientes obtiennent une erreur de certificat, envoyez les modifications après avoir généré ou chargé le certificat racine dans Secure Web Appliance, puis distribuez le certificat aux machines clientes et validez les modifications sur l'appliance.

Gestion de la validation et du déchiffrement des certificats pour HTTPS

Secure Web Appliance valide les certificats avant d'inspecter et de déchiffrer le contenu.

Certificats valides

Qualités d'un certificat valide :

- **Non expiré.** La période de validité du certificat inclut la date du jour courant.
- **Autorité de certification reconnue.** L'autorité de certification émettrice est incluse dans la liste des autorités de certification approuvées stockée sur Secure Web Appliance.
- **Signature valide.** La signature numérique a été correctement mise en œuvre selon des normes cryptographiques.
- **Des noms uniformes.** Le nom commun correspond au nom d'hôte spécifié dans l'en-tête HTTP.
- **Non révoqué.** L'autorité de certification émettrice n'a pas révoqué le certificat.

Thèmes connexes

- Activation de la vérification de l'état de révocation en temps réel, on page 292
- Configuration du traitement des certificats non valides, on page 291
- Options de vérification de l'état de révocation des certificats, on page 291

Traitement des certificats non valides

L'appliance peut effectuer l'une des actions suivantes pour les certificats de serveur non valides :

- **Drop.**
- **Decrypt.**
- **Supervision.**

Certificats non valides pour plusieurs raisons

Pour les certificats de serveur qui ne sont pas valides en raison d'une autorité racine non reconnue et d'un certificat expiré, le proxy HTTPS effectue l'action qui s'applique aux autorités racine non reconnues.

Dans tous les autres cas, pour les certificats de serveur qui ne sont pas valides pour plusieurs raisons à la fois, le proxy HTTPS effectue les actions dans l'ordre, de la plus restrictive à la moins restrictive.

Avertissements de certificat non fiable pour les connexions déchiffrées

Lorsque Secure Web Appliance rencontre un certificat non valide et est configuré pour déchiffrer la connexion, AsyncOS crée un certificat non fiable qui exige que l'utilisateur final accepte ou rejette la connexion. Le nom commun du certificat est « Untrusted Certificate Warning » (Avertissement de certificat non fiable).

L'ajout de ce certificat non approuvé à la liste des certificats approuvés supprimera la possibilité pour l'utilisateur final d'accepter ou de rejeter la connexion.

Quand AsyncOS génère l'un de ces certificats, il crée une entrée de journal de proxy avec le texte « Signing untrusted key » ou « Signing untrusted cert » (Signature d'une clé non approuvée) ou « Signing untrusted cert » (Signature de certificat non approuvé).

Chargement d'un certificat racine et d'une clé

Before you begin

Activez le proxy HTTPS. Activation du proxy HTTPS, on page 283.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Use Uploaded Certificate and Key** (Utiliser le certificat et la clé téléchargés).

Étape 4 Cliquez sur **Browse** (Parcourir) dans le champ Certificate (Certificat) pour naviguer jusqu'au fichier de certificat stocké sur l'ordinateur local.

Si le fichier que vous téléchargez contient plusieurs certificats ou clés, le proxy Web utilise le premier certificat ou la première clé du fichier.

Étape 5 Cliquez sur **Browse** (Parcourir) dans le champ Key (Clé) pour accéder au fichier de clé privée.

Note La longueur de la clé doit être de 512, 1024 ou 2048 bits.

Étape 6 Sélectionnez **Key is Encrypted** (La clé est chiffrée) si la clé est chiffrée.

Étape 7 Cliquez sur **Upload Files** (Charger les fichiers) pour transférer le certificat et les fichiers de clé vers Secure Web Appliance.

Les informations sur le certificat chargé sont affichées sur la page Edit HTTPS Proxy Settings (Modifier les paramètres de proxy HTTPS).

Étape 8 (Facultatif) Cliquez sur **Download Certificate** (Télécharger le certificat) afin de pouvoir le transférer vers les applications clientes sur le réseau.

Étape 9 Envoyez et validez vos modifications.

Génération d'un certificat et d'une clé pour le proxy HTTPS

Before you begin

Activez le proxy HTTPS. Activation du proxy HTTPS, on page 283.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Use Generate Certificate and Key** (Utiliser le certificat et la clé générés).

Étape 4 Cliquez sur **Generate New Certificate and Key** (Générer un nouveau certificat et une nouvelle clé).

Étape 5 Dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé), saisissez les informations à afficher dans le certificat racine.

Vous pouvez saisir n'importe quel caractère ASCII, à l'exception de la barre oblique (/) dans le champ **Common Name** (Nom commun).

Étape 6 Cliquez sur **Generate** (Générer).

Étape 7 Les informations sur le certificat généré sont affichées sur la page Edit HTTPS Proxy Settings (Modifier les paramètres de proxy HTTPS).

Étape 8 (Facultatif) Cliquez sur **Download Certificate** (Télécharger le certificat) afin de pouvoir le transférer vers les applications clientes sur le réseau.

Étape 9 (Facultatif) Cliquez sur le lien **Download Certificate Signing Request** (Télécharger la requête de signature de certificat) afin de pouvoir envoyer la requête de signature de certificat (CSR) à une autorité de certification (CA).

Étape 10 (Facultatif) Après avoir reçu le certificat signé de l'autorité de certification, chargez-le dans Secure Web Appliance. Vous pouvez le faire à tout moment après avoir généré le certificat sur l'appliance.

Étape 11 Envoyez et validez les modifications.

Configuration du traitement des certificats non valides

Before you begin

Vérifiez que le proxy HTTPS est activé, comme décrit dans Activation du proxy HTTPS, on page 283.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Pour chaque type d'erreur de certificat, définissez la réponse du proxy : **Drop**, **Decrypt**, or **Monitor**.

Type d'erreur de certificat	Description
Expiré	La date actuelle se trouve en dehors de la plage de validité du certificat.
Nom d'hôte non concordant	Le nom d'hôte dans le certificat ne correspond pas au nom d'hôte auquel le client tentait d'accéder. **Note** Le proxy Web ne peut effectuer une correspondance de nom d'hôte que s'il est déployé en mode de transfert explicite. Lorsqu'il est déployé en mode transparent, il ne connaît pas le nom d'hôte du serveur de destination (il ne connaît que l'adresse IP). Il ne peut donc pas le comparer au nom d'hôte indiqué dans le certificat du serveur.
Autorité racine/émetteur non reconnu	L'autorité racine ou une autorité de certification intermédiaire n'est pas reconnue.
Certificat de signature non valide	Il y a eu un problème avec le certificat de signature.
Certificat feuille non valide	Un problème est survenu avec le certificat feuille, notamment un problème de rejet, de décodage ou de non-concordance.
Tous les autres types d'erreurs	La plupart des autres types d'erreurs sont dues au fait que l'appliance n'est pas en mesure d'établir la liaison SSL avec le serveur HTTPS. Pour de plus amples renseignements sur d'autres scénarios d'erreur liés aux certificats de serveur, consultez l'adresse http://www.openssl.org/docs/apps/verify.html.

Étape 4 Envoyez et validez les modifications.

Options de vérification de l'état de révocation des certificats

Pour déterminer si l'autorité de certification émettrice a révoqué un certificat, Secure Web Appliance peut effectuer une vérification auprès de l'autorité de certification émettrice des manières suivantes :

- **Liste de révocation de certificat (certificats Comodo uniquement)** Secure Web Appliance vérifie la liste de révocation des certificats de Comodo. Comodo gère cette liste et la met à jour en fonction de ses propres politiques. Selon la date de la dernière mise à jour, la liste de révocation des certificats peut être obsolète au moment de la vérification par Secure Web Appliance.
- **Protocole d'état du certificat en ligne (OCSP).** Secure Web Appliance vérifie l'état de révocation auprès de l'autorité de certification émettrice en temps réel. Si l'autorité de certification émettrice prend

en charge OCSP, le certificat contient une URL pour la vérification de l'état en temps réel. Cette fonctionnalité est activée par défaut pour les nouvelles installations et désactivée par défaut pour les mises à jour.

Note Secure Web Appliance effectue l'interrogation OCSP uniquement pour les certificats qu'il juge valides à tous les autres égards et qui comprennent l'URL OCSP.

Thèmes connexes

- Activation de la vérification de l'état de révocation en temps réel, on page 292
- Configuration du traitement des certificats non valides, on page 291

Activation de la vérification de l'état de révocation en temps réel

Before you begin

Assurez-vous que le proxy HTTPS est activé. Consultez Activation du proxy HTTPS, on page 283.

Étape 1 **Security Services > HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Enable Online Certificate Status Protocol (OCSP)** [Activer le protocole d'état du certificat en ligne (OCSP)].

Étape 4 Configurez les propriétés de **OCSP Result Handling** (Gestion des résultats OCSP).

Cisco recommande de configurer les options de gestion des résultats OCSP sur les mêmes actions que les options de gestion des certificats non valides. Par exemple, si vous renseignez Expired Certificate (Certificat expiré) par Monitor (Superviser), définissez le certificat révoqué sur Monitor (Superviser).

Étape 5 (Facultatif) Développez la section Advanced configuration (Configuration avancée) et configurez les paramètres décrits ci-dessous.

Nom du champ	Description
OCSP Valid Response Cache Timeout (Délai d'expiration du cache de réponse valide OCSP)	Temps d'attente avant de revérifier une réponse OCSP valide en secondes (s), minutes (m), heures (h) ou jours (d). L'unité par défaut est seconde. La plage valide est comprise entre 1 seconde et 7 jours.
OCSP Invalid Response Cache Timeout (Délai d'expiration du cache de réponse OCSP non valide)	Temps d'attente avant de revérifier une réponse OCSP non valide en secondes (s), minutes (m), heures (h) ou jours (d). L'unité par défaut est seconde. La plage valide est comprise entre 1 seconde et 7 jours.

Nom du champ	Description
OCSP Network Error Cache Timeout (Délai d'expiration du cache d'erreur de réseau OCSP)	Temps d'attente avant de tenter de contacter à nouveau le répondeur OCSP après avoir échoué à obtenir une réponse, en secondes (s), minutes (m), heures (h) ou jours (d). Plage valide comprise entre 1 seconde et 24 heures.
Allowed Clock Skew (Décalage d'horloge autorisé)	Différence maximale autorisée dans les paramètres de temps entre le Secure Web Appliance et le répondeur OCSP, en secondes (s) ou en minutes (m). Plage valide comprise entre 1 seconde et 60 minutes.
Maximum Time to Wait for OCSP Response (Temps d'attente maximal d'une réponse OCSP)	Temps maximal d'attente d'une réponse du répondeur OCSP. La plage valide est comprise entre 1 seconde et 10 minutes. Indiquez une durée plus courte pour réduire les délais d'accès de l'utilisateur final aux requêtes HTTPS au cas où le répondeur OCSP ne serait pas disponible.
Use upstream proxy for OCSP checking (Utiliser un proxy en amont pour la vérification OCSP)	Nom de groupe des proxys en amont.
Servers exempt from upstream proxy (Serveurs dispensés du proxy en amont)	Adresses IP ou noms d'hôte des serveurs à exclure. Peut être laissé vide.

Étape 6 Envoyez et validez les modifications.

Certificats racine approuvés

Le Secure Web Appliance est livré avec et gère une liste de certificats racine approuvés. Les sites Web dotés de certificats approuvés n'ont pas besoin de déchiffrement.

Vous pouvez gérer la liste des certificats approuvés, en y ajoutant et en en supprimant fonctionnellement des certificats. Bien que Secure Web Appliance ne supprime pas les certificats de la liste principale, il vous permet de remplacer la confiance dans un certificat, ce qui supprime fonctionnellement le certificat de la liste approuvée.

Ajout de certificats à la liste approuvée

Before you begin

Vérifiez que le proxy HTTPS est activé. Consultez Activation du proxy HTTPS, on page 283.

Étape 1 **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Manage Trusted Root Certificates** (Gérer les certificats racine approuvés).

Étape 3 Cliquez sur **Import** (Importer).

Étape 4 Cliquez sur **Browse** (Parcourir) et accédez au fichier de certificat.

Étape 5 **Envoyez** et **validez** les modifications.

Recherchez le certificat que vous avez téléchargé dans la liste **Custom Trusted Root Certificates** (Certificats racine approuvés personnalisés).

Suppression de certificats de la liste approuvée

Étape 1 Sélectionnez **Security Services** > **HTTPS Proxy** (Services de sécurité > Proxy HTTPS).

Étape 2 Cliquez sur **Manage Trusted Root Certificates** (Gérer les certificats racine approuvés).

Étape 3 Cochez la case **Override Trust** (Remplacer la confiance) correspondant au certificat que vous souhaitez supprimer de la liste.

Étape 4 **Envoyez** et **validez** les modifications.

Routage du trafic HTTPS

La capacité d'AsyncOS à acheminer les transactions HTTPS en fonction des informations stockées dans les en-têtes des clients est limitée et différente pour le HTTPS transparent et explicite.

Option	Description
Transparent HTTPS (HTTPS transparent)	Dans le cas d'un HTTPS transparent, AsyncOS n'a pas accès aux informations dans les en-têtes du client. Par conséquent, AsyncOS ne peut pas appliquer les politiques de routage si une politique de routage ou un profil d'identification repose sur les informations contenues dans les en-têtes de client.
Explicit HTTPS (HTTPS explicite)	Dans le cas d'un protocole HTTPS explicite, AsyncOS a accès aux informations suivantes dans les en-têtes des clients : • URL • Numéro du port de destination Par conséquent, pour les transactions HTTPS explicites, il est possible de mettre en correspondance une politique de routage basée sur l'URL ou le numéro de port.

Résolution de problèmes relatifs aux déchiffrement/HTTPS/certificats

- Accès aux sites HTTPS à l'aide de politiques de routage avec critères de catégorie d'URL, on page 642
- HTTPS avec substituts basés sur IP et demandes transparentes, on page 642
- Contournement du déchiffrement pour des sites Web particuliers, on page 643
- Alerte : Problème lié au certificat de sécurité, on page 644

CHAPITRE 12

Analyser le trafic sortant à la recherche d'infections existantes

Cette rubrique contient les sections suivantes :

Survol de l'analyse du trafic sortant

Pour empêcher des données malveillantes de quitter le réseau, le Secure Web Appliance fournit la fonctionnalité d'analyse des programmes malveillants sortants. Les groupes de politiques vous permettent de définir quels téléchargements sont analysés à la recherche de programmes malveillants, quels moteurs d'analyse utiliser pour l'analyse et quels types de programmes malveillants bloquer.

Le moteur de conversion en flux continu et vecteur dynamique de Cisco (DVS) analyse les demandes de transaction dès qu'elles quittent le réseau. En fonctionnant avec le moteur Cisco DVS, le Secure Web Appliance vous permet d'empêcher les utilisateurs de charger involontairement des données malveillantes.

Vous pouvez effectuer les tâches suivantes:

Tâche	Lien vers la tâche
Créer des politiques pour bloquer les programmes malveillants	Création de politiques d'analyse à la recherche de programmes malveillants sortants, on page 297
Affecter des demandes de téléchargement aux groupes de politiques sur les programmes malveillants sortants	Contrôle des demandes de chargement , on page 299

Expérience de l'utilisateur lorsque les demandes sont bloquées par le moteur DVS

Lorsque le moteur Cisco DVS bloque une demande de chargement, le proxy Web envoie une page de blocage à l'utilisateur final. Cependant, tous les sites Web n'affichent pas la page de blocage à l'utilisateur final. Certains sites Web 2.0 affichent du contenu dynamique en utilisant Javascript au lieu d'une page Web statique et il est peu probable qu'ils affichent la page de blocage. Les utilisateurs sont toujours correctement empêchés de charger des données malveillantes, mais ils ne sont pas toujours informés par le site Web.

Interprétation des demandes de chargement

Les politiques d'analyse des programmes malveillants sortants définissent si le proxy Web bloque les requêtes HTTP et les connexions HTTPS déchiffrées pour les transactions qui téléchargent des données vers un serveur (demandes de téléchargement). Une demande de téléchargement est une demande HTTP ou HTTPS déchiffré dont le corps a du contenu.

Lorsque le proxy Web reçoit une demande de téléchargement, il la compare aux groupes de politiques des groupes de politiques d'analyse des programmes malveillants sortants afin de déterminer le groupe de politiques à appliquer. Après avoir affecté la demande à un groupe de politiques, il compare la demande aux paramètres de contrôle configurés du groupe de politiques pour déterminer s'il faut bloquer la demande ou surveiller la demande. Lorsqu'une politique d'analyse des programmes malveillants sortants détermine la supervision d'une demande, celle-ci est évaluée par rapport aux politiques d'accès, et l'action finale implémentée par le proxy Web sur la demande est déterminée par la politique d'accès.

Note Les demandes de téléchargement qui tentent de charger des fichiers d'une taille de zéro (0) octet ne sont pas évaluées par rapport aux politiques d'analyse des programmes malveillants sortants.

Critères d'appartenance à un groupe

Chaque demande client est affectée à une identité et est ensuite évaluée par rapport aux autres types de politiques afin de déterminer à quel groupe de politiques elle appartient pour chaque type. Le proxy Web applique les paramètres de contrôle de politiques configurés à une demande d'un client en fonction de l'appartenance au groupe de politiques de la demande.

Le proxy Web suit un processus précis pour correspondre aux critères d'appartenance au groupe. Il prend en compte les facteurs suivants pour l'appartenance à un groupe :

Critère	Description
Identification Profile (Profil d'identification)	Chaque demande de client correspond à un **profil d'identification**, échoue à l'authentification et obtient l'accès invité, ou échoue à l'authentification et est terminée.

Critère	Description
Authorized users (Utilisateurs autorisés).	Si le **profil d'identification** attribué nécessite une authentification, l'utilisateur doit être dans la liste des utilisateurs autorisés dans le groupe de politiques de l'analyse des programmes malveillants sortants pour correspondre au groupe de politiques. La liste d'utilisateurs autorisés peut comprendre n'importe quel groupe ou utilisateur précisé ou peut être des utilisateurs invités si le **profil d'identification** permet l'accès comme invité.
Advanced options (Options avancées)	Vous pouvez configurer plusieurs options avancées pour l'appartenance au groupe de politiques d'analyse des programmes malveillants sortants. Certaines options, telles que le port proxy et la catégorie d'URL, peuvent également être définies dans le **profil d'identification**. Lorsqu'une option avancée est configurée dans le **profil d'identification**, elle n'est pas configurable au niveau de groupe de la Politique d'analyse des programmes malveillants sortants.

Mise en correspondance des demandes des clients et des groupes de politiques d'analyse à la recherche de programmes malveillants sortants

Le proxy Web compare l'état de la demande de chargement aux critères d'appartenance au premier groupe de politiques. S'ils correspondent, le proxy Web applique les paramètres de politique de ce groupe de politiques.

S'ils ne correspondent pas, le proxy Web compare la demande de chargement au groupe de politiques suivant. Il poursuit ce processus jusqu'à ce qu'il fasse correspondre la demande de chargement à un groupe de politiques défini par l'utilisateur. S'il ne correspond pas à un groupe de politiques défini par l'utilisateur, il correspond au groupe de politiques global. Lorsque le proxy Web fait correspondre la demande de chargement à un groupe de politiques ou au groupe de politiques global, il applique les paramètres de politiques de ce groupe de politiques.

Création de politiques d'analyse à la recherche de programmes malveillants sortants

Vous pouvez créer des groupes de politiques d'analyse des programmes malveillants sortants en fonction de combinaisons de plusieurs critères, comme une ou plusieurs identités ou la catégorie d'URL du site de destination. Vous devez définir au moins un critère d'appartenance à un groupe de politiques. Lorsque vous définissez plusieurs critères, la demande de chargement doit satisfaire à tous les critères pour correspondre au groupe de politiques. Cependant, la demande de chargement ne doit correspondre qu'à l'une des identités configurées.

Étape 1 Choisissez **Web Security Manager > Outbound Malware Scanning** (Web Security Manager > Analyse des programmes malveillants sortants).

Étape 2 Cliquez sur **Add Policy** (Ajouter une politique).

Étape 3 Saisissez un nom et une description facultative pour le groupe de politiques.

Note Chaque nom de groupe de politiques doit être unique et contenir uniquement des caractères alphanumériques ou un espace.

Étape 4 Dans le champ Insert Above Policy (Insérer au-dessus de la politique), sélectionnez l'emplacement dans le tableau des politiques où insérer le groupe de politiques.

Lors de la configuration de plusieurs groupes de politiques, vous devez préciser un ordre logique pour chaque groupe.

Étape 5 Dans la section **Identification Profiles and Users** (Profils d'identification et utilisateurs), sélectionnez un ou plusieurs groupes d'identité à appliquer à ce groupe de politiques.

Étape 6 (Facultatif) Développez la section « Advanced » (Avancé) pour définir les exigences d'appartenance supplémentaires.

Étape 7 Pour définir l'appartenance à un groupe de politiques en fonction des options avancées, cliquez sur le lien de l'option avancée et configurez l'option dans la page qui s'affiche.

Option avancée	Description
Protocols (Protocoles)	Choisissez de définir ou non l'appartenance au groupe de politiques par le protocole utilisé dans la demande du client. Sélectionnez les protocoles à inclure. « All others » (Tous les autres) désigne tout protocole non répertorié au-dessus de cette option. **Note** Lorsque le proxy HTTPS est activé, seules les politiques de déchiffrement s'appliquent aux transactions HTTPS. Vous ne pouvez pas définir l'appartenance aux politiques à l'aide du protocole HTTPS pour les politiques d'accès, de routage, d'analyse des programmes malveillants sortants, de sécurité des données ou DLP externes.
Proxy Ports (Ports du proxy)	Choisissez de définir ou non l'appartenance au groupe de politiques par le port de proxy utilisé pour accéder au proxy Web. Entrez un ou plusieurs numéros de port dans le champ Proxy Ports (Ports du proxy). Séparez les valeurs de ports multiples par des virgules. Pour les connexions de transfert explicite, il s'agit du port configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination. Si vous définissez l'appartenance à un groupe de politiques par le port proxy lorsque les demandes des clients sont redirigées de manière transparente vers l'appliance, certaines demandes peuvent être refusées. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques autre que l'identité.
Subnets (Sous-réseaux)	Choisissez de définir ou non l'appartenance au groupe de politiques par sous-réseau ou autres adresses. Vous pouvez choisir d'utiliser les adresses qui peuvent être définies avec l'identité associée ou vous pouvez entrer des adresses spécifiques ici. **Note** Si l'identité associée à ce groupe de politiques définit ses membres par des adresses, alors vous devez saisir dans ce groupe de politiques des adresses qui sont un sous-ensemble des adresses définies dans l'identité. L'ajout d'adresses dans le groupe de politiques réduit davantage la liste des transactions qui correspondent à ce groupe de politiques.
URL Categories (Catégories d'URL)	Choisissez de définir ou non l'appartenance au groupe de politiques par catégories d'URL. Sélectionnez les catégories d'URL prédéfinies ou définies par l'utilisateur. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques autre que l'identité.

Option avancée	Description
User Agents (Agents utilisateur)	Choisissez si vous souhaitez définir l'appartenance au groupe de politiques en fonction des agents utilisateur (applications clientes telles que les programmes de mise à jour et les navigateurs Web) utilisés dans la demande du client. Vous pouvez sélectionner des agents utilisateur couramment définis ou définir les vôtres à l'aide d'expressions régulières. Indique si la définition d'appartenance inclut uniquement les agents utilisateur sélectionnés ou exclut expressément les agents utilisateur sélectionnés. **Note** Si le **profil d'identification** associé à ce groupe de politiques définit l'appartenance au **profil d'identification** en fonction de ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques sans **profil d'identification**.
User Location (Emplacement de l'utilisateur)	Choisissez de définir ou non l'appartenance au groupe de politiques par emplacement d'utilisateur, distant ou local.

Étape 8 Envoyez vos modifications.

Étape 9 Configurez les paramètres de contrôle de groupe de la politique d'analyse des programmes malveillants sortants pour définir la façon dont le proxy Web gère les transactions.

Le nouveau groupe de politiques d'analyse des programmes malveillants sortants hérite automatiquement des paramètres globaux du groupe de politiques jusqu'à ce que vous configuriez des options pour chaque paramètre de contrôle.

Étape 10 Envoyez et validez les modifications.

Contrôle des demandes de chargement

Chaque demande de téléchargement est affectée à un groupe de politiques d'analyse des programmes malveillants sortants et hérite des paramètres de contrôle de ce groupe de politiques. Une fois que le proxy Web a reçu les en-têtes de la demande de chargement, il dispose des informations nécessaires pour décider s'il doit analyser le corps de la demande. Le moteur DVS analyse la demande et renvoie un verdict au proxy Web. La page de blocage s'affiche pour l'utilisateur final, le cas échéant.

Étape 1 Choisissez **Web Security Manager > Outbound Malware Scanning** (Web Security Manager > Analyse des programmes malveillants sortants).

Étape 2 Dans la colonne **Destinations**, cliquez sur le lien correspondant au groupe de politiques que vous souhaitez configurer.

Étape 3 Dans la section **Edit Destination Settings** (Modifier les paramètres de destination), sélectionnez **Define Destinations Scanning Custom Settings** (Définir les paramètres personnalisés d'analyse de destination) dans le menu déroulant.

Étape 4 Dans la section **Destinations to Scan** (Destinations à analyser), sélectionnez l'une des options suivantes :

Option	Description
Do not scan any uploads (Ne pas analyser les téléchargements)	Le moteur DVS n'analyse aucune demande de téléchargement. Toutes les demandes de téléchargement sont évaluées par rapport aux politiques d'accès

Option	Description
Scan all uploads (Analyser tous les chargements)	Le moteur DVS analyse toutes les demandes de téléchargement. La demande de téléchargement est bloquée ou évaluée par rapport aux politiques d'accès, selon le verdict d'analyse du moteur DVS
Scan uploads to specified custom URL categories (Analyser les téléchargements vers des catégories d'URL personnalisées précisées)	Le moteur DVS analyse les demandes de chargement qui appartiennent à des catégories d'URL personnalisées spécifiques. La demande de téléchargement est bloquée ou évaluée par rapport aux politiques d'accès, selon le verdict d'analyse du moteur DVS. Cliquer sur **Edit custom categories list** (Modifier la liste des catégories personnalisées) pour sélectionner les catégories d'URL à analyser.

Étape 5 Envoyez vos modifications.

Étape 6 Dans la colonne **Anti-Malware Filtering** (Filtrage des programmes malveillants), cliquez sur le lien du groupe de politiques.

Étape 7 Dans la section **Anti-Malware Settings** (Paramètres de protection contre les programmes malveillants), sélectionnez **Define Anti-Malware Custom Settings** (Définir les paramètres personnalisés de la protection contre les programmes malveillants).

Étape 8 Dans la section **Cisco DVS Anti-Malware Settings** (Paramètres de protection contre les programmes malveillants Cisco DVS), sélectionnez les moteurs d'analyse de protection contre les programmes malveillants à activer pour ce groupe de politiques.

Étape 9 Dans la section **Malware Catégories** (Catégories de programmes malveillants), sélectionnez si vous souhaitez surveiller ou bloquer les différentes catégories de programmes malveillants.

Les catégories répertoriées dans cette section dépendent des moteurs d'analyse que vous activez.

Note Les transactions URL sont classées comme non analysables lorsque le paramètre de durée maximale configuré est atteint ou lorsque le système éprouve une condition d'erreur transitoire. Par exemple, les transactions peuvent être classées comme non analysables lors des mises à jour du moteur d'analyse ou des mises à niveau d'AsyncOS. Les verdicts d'analyse des programmes malveillants SV_TIMEOUT et SV_ERROR sont considérés comme des transactions non analysables.

Étape 10 Envoyez et validez les modifications.

Journalisation de l'analyse DVS

Les journaux d'accès indiquent si le moteur DVS a analysé ou non une demande de téléchargement à la recherche de programmes malveillants. La section du verdict d'analyse de chaque entrée du journal des accès comprend des valeurs pour l'activité du moteur DVS pour les téléchargements analysés. Vous pouvez également ajouter l'un des champs aux journaux d'accès ou W3C pour trouver plus facilement l'activité de ce moteur DVS :

Table 6: Champs de journalisation dans les journaux W3C et spécificateurs de format dans les journaux d'accès

Champ de journalisation W3C	Spécificateur de format dans les journaux d'accès
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4

Champ de journalisation W3C	Spécificateur de format dans les journaux d'accès
x-req-dvs-verdictname	%X3

Lorsque le moteur DVS marque une demande de téléchargement comme étant un programme malveillant et qu'il est configuré pour bloquer les téléchargements de programmes malveillants, la balise de décision ACL dans les journaux d'accès est BLOCK_AMW_REQ.

Cependant, lorsque le moteur DVS marque une demande de téléchargement comme étant un programme malveillant et qu'il est configuré pour *surveiller* les téléchargements de programmes malveillants, la balise de décision dans les journaux d'accès est en fait déterminée par la politique d'accès appliquée à la transaction.

Pour déterminer si le moteur DVS a analysé une demande de téléchargement à la recherche de programmes malveillants, affichez les résultats de l'activité du moteur DVS dans la section des renseignements sur le verdict d'analyse de chaque entrée du journal des accès.

CHAPITRE 13

Configuration des services de sécurité

Cette rubrique contient les sections suivantes :

Survol de la configuration des services de sécurité

Secure Web Appliance utilise des composants de sécurité pour protéger les utilisateurs finaux contre un éventail de programmes malveillants. Vous pouvez configurer les paramètres de protection contre les programmes malveillants et de réputation de sites Web pour chaque groupe de politiques. Lorsque vous configurez des politiques d'accès, AsyncOS pour le Web peut également choisir une combinaison d'analyses de protection contre les programmes malveillants et d'évaluation de réputation Web à utiliser pour déterminer le contenu à bloquer.

Pour protéger les utilisateurs finaux contre les programmes malveillants, vous activez ces fonctionnalités sur l'appliance, puis configurez les paramètres de protection contre les programmes malveillants et de réputation Web conformément à la politique.

Option	Description	Lien
Anti-malware scanning (Analyse de protection contre les programmes malveillants)	Fonctionne avec plusieurs moteurs d'analyse de protection contre les programmes malveillants intégrés à l'appliance pour bloquer les programmes malveillants	Survol de l'analyse à la recherche de programmes malveillants , on page 307

Option	Description	Lien
Web Reputation Filters (Filtres de réputation Web)	Analyse le comportement du serveur Web et détermine si l'URL contient un programme malveillant basé sur l'URL	Survol des filtres de réputation Web , on page 304
Cisco Secure Endpoint	Protection contre les menaces dans les fichiers téléchargés en évaluant la réputation des fichiers et en analysant les caractéristiques des fichiers.	Survol du filtrage de réputation de fichiers et de l'analyse de fichiers , on page 323

Thèmes connexes

- Activation des filtres contre les programmes malveillants et de réputation, on page 310
- Interprétation de l'analyse adaptative, on page 309

Survol des filtres de réputation Web

Les filtres de réputation Web attribuent un score de réputation Web (WBRS) à une URL pour déterminer la probabilité qu'elle contienne des programmes malveillants basés sur l'URL. Le Secure Web Appliance utilise les scores de réputation Web pour identifier et arrêter les attaques de programmes malveillants avant qu'elles ne se produisent. Vous pouvez utiliser des filtres de réputation Web avec les politiques d'accès, de déchiffrement et de sécurité des données de Cisco.

Score de réputation Web

Les filtres de réputation Web utilisent des données pour évaluer la fiabilité des domaines Internet et la réputation des URL. Le calcul de la réputation Web associe une URL à des paramètres réseau pour déterminer la probabilité que des programmes malveillants soient présents. La probabilité agrégée de la présence de programmes malveillants est ensuite mappée sur un indice de réputation Web compris entre -10 et +10, +10 étant la valeur la moins susceptible de contenir des programmes malveillants.

Voici des exemples de paramètres :

- Données de catégorisation d'URL
- Présence d'un code téléchargeable
- Présence de contrats de licence d'utilisateur final (CLUF) longs et brouillés
- Volume global et variations de volume
- Renseignements sur le propriétaire du réseau
- Historique d'une URL
- Âge d'une URL
- Présence sur toutes les listes de blocage
- Présence sur toutes les listes d'autorisation
- Fautes de frappe d'URL de domaines populaires
- Informations sur le bureau d'enregistrement de domaine
- Informations sur l'adresse IP

Note Cisco ne recueille pas de renseignements permettant d'identifier les clients, comme les noms d'utilisateur, les phrases secrètes ou les adresses IP des clients.

Comprendre le fonctionnement du filtrage de réputation Web

Les scores de réputation Web sont associés à une action à effectuer sur une demande d'URL. Vous pouvez configurer chaque groupe de politiques pour corréler une action à un score de réputation Web particulier. Les actions disponibles dépendent du type de groupe de politiques affecté à la demande d'URL :

Type de politique	Action
Politiques d'accès	Vous pouvez choisir de bloquer, d'analyser ou d'autoriser
Politiques de déchiffrement	Vous pouvez choisir d'abandonner, de déchiffrer ou de transmettre
Politiques de sécurité des données de Cisco	Vous pouvez choisir de bloquer ou de surveiller

Réputation Web dans les politiques d'accès

Lorsque vous configurez les paramètres de réputation Web dans les politiques d'accès, vous pouvez choisir de les configurer manuellement ou de laisser AsyncOS pour le Web choisir les meilleures options à l'aide de l'analyse adaptative. Lorsque l'analyse adaptative est activée, vous pouvez activer ou désactiver le filtrage de réputation Web dans chaque politique d'accès, mais vous ne pouvez pas modifier les scores de réputation Web.

Résultat	Action	Description	Exemple
-10 à -6,0	Block (Bloquer)	Mauvais site. La demande est bloquée et aucune autre analyse contre les programmes malveillants ne se produit.	• L'URL télécharge des informations sans l'autorisation de l'utilisateur. • Pointe subite du volume d'URL. • L'URL correspond à un domaine populaire avec une faute de frappe.
-5,9 à 5,9	Analyser	Site indéterminé. La demande est transmise au moteur DVS pour une analyse plus poussée des programmes malveillants. Le moteur DVS analyse le contenu de la demande et de la réponse du serveur.	• URL créée récemment qui a une adresse IP dynamique et qui contient du contenu téléchargeable. • Adresse IP de propriétaire du réseau ayant un score de réputation Web positif.

Résultat	Action	Description	Exemple
6,0 à 10,0	Allow (Autoriser)	Bon site. La demande est autorisée. Aucune analyse des programmes malveillants requise.	• L'URL ne comporte aucun contenu téléchargeable. • Domaine réputé, à volume élevé, existant depuis longtemps. • Domaine présent sur plusieurs listes d'autorisation. • Aucun lien vers des URL de mauvaise réputation.

Par défaut, les URL d'une requête HTTP auxquelles un score de réputation de sites Web supérieur ou égal à 7 est attribué sont autorisées et ne nécessitent pas d'analyse supplémentaire. Cependant, un score plus faible pour une demande HTTP, tel que 3 ou plus, est automatiquement transféré au moteur Cisco DVS où il est analysé afin de détecter les programmes malveillants. Toute URL dans une demande HTTP qui a une mauvaise réputation est bloquée.

Thèmes connexes

- Interprétation de l'analyse adaptative, on page 309

Réputation Web dans les politiques de déchiffrement

Résultat	Action	Description
-10 à -9,0	Abandonner	Mauvais site. La demande est abandonnée sans avis envoyé à l'utilisateur final. Utilisez ce paramètre avec prudence.
-8,9 à 5,9	Déchiffrer	Site indéterminé. La demande est autorisée, mais la connexion est déchiffrée, et des politiques d'accès sont appliquées au trafic déchiffré.
6,0 à 10,0	Intercommunication	Bon site. La demande est transmise sans inspection ni déchiffrement.

Réputation Web dans les politiques de sécurité des données de Cisco

Résultat	Action	Description
-10 à -6,0	Block (Bloquer)	Mauvais site. La transaction est bloquée et aucune autre analyse n'est effectuée.
-5,9 à 0,0	Monitor (Surperviser)	La transaction ne sera pas bloquée en fonction de la réputation Web et fera l'objet d'une vérification de contenu (type et taille de fichier). **Note** Les sites sans score de réputation sont surveillés.

Survol de l'analyse à la recherche de programmes malveillants

La fonction de protection contre les programmes malveillants Secure Web Appliance utilise le moteur Cisco DVS™ en combinaison avec des moteurs d'analyse de protection contre les programmes malveillants pour bloquer les menaces contre les programmes malveillants sur le Web. Le moteur DVS fonctionne avec les moteurs d'analyse de protection contre les programmes malveillants Webroot™, McAfee et Sophos.

Les moteurs d'analyse inspectent les transactions pour déterminer un verdict d'analyse des programmes malveillants à transmettre au moteur DVS. Le moteur DVS détermine s'il faut surveiller ou bloquer la demande en fonction des verdicts de l'analyse des programmes malveillants. Pour utiliser le composant de protection contre les programmes malveillants de l'appliance, vous devez activer l'analyse contre les programmes malveillants et configurer les paramètres globaux, puis appliquer des paramètres spécifiques à différentes politiques.

Thèmes connexes

- Activation des filtres contre les programmes malveillants et de réputation, on page 310
- Interprétation de l'analyse adaptative, on page 309
- Analyse McAfee, on page 308

Comprendre le fonctionnement du moteur DVS

Le moteur DVS effectue une analyse de protection contre les programmes malveillants sur les transactions URL transférées à partir des filtres de réputation Web. Les filtres de réputation Web calculent la probabilité qu'une URL particulière contienne un programme malveillant et attribuent un score d'URL associé à une action pour bloquer, analyser ou autoriser la transaction.

Lorsque le score de réputation attribué indique d'analyser la transaction, le moteur DVS reçoit la demande d'URL et le contenu de la réponse du serveur. Le moteur DVS, en combinaison avec les moteurs d'analyse Webroot et/ou Sophos ou McAfee, renvoie un verdict d'analyse de programmes malveillants. Le moteur DVS utilise les informations des verdicts de recherche de programmes malveillants et des paramètres de politique d'accès pour déterminer s'il faut bloquer ou transmettre le contenu au client.

Utilisation de plusieurs verdicts de programmes malveillants

Le moteur DVS peut déterminer plusieurs verdicts de programmes malveillants pour une seule URL. Plusieurs verdicts peuvent émaner d'un des moteurs d'analyse activés ou des deux :

- **Différents verdicts émanant de différents moteurs d'analyse.** Lorsque vous activez Webroot et Sophos ou McAfee, chaque moteur d'analyse peut renvoyer différents verdicts de programmes malveillants pour le même objet. Lorsqu'une URL entraîne plusieurs verdicts de la part des deux moteurs d'analyse activés, l'appliance effectue l'action la plus restrictive. Par exemple, si un moteur d'analyse renvoie un verdict de blocage et l'autre un verdict de supervision, le moteur DVS bloque toujours la demande.
- **Différents verdicts émanant du même moteur d'analyse.** Un moteur d'analyse peut renvoyer plusieurs verdicts pour un seul objet lorsque ce dernier contient plusieurs infections. Lorsqu'une URL entraîne plusieurs verdicts de la part du même moteur d'analyse, l'appliance prend des mesures en fonction du verdict ayant la priorité la plus élevée. Le texte suivant répertorie les verdicts possibles d'analyse de programmes malveillants, de la priorité la plus élevée à la plus faible.
- Virus

- Outil de téléchargement de chevaux de Troie
- Cheval de Troie
- Cheval de Troie pour hameçonnage
- Détournement d'identité
- Supervision du système
- Supervision de système commercial
- Composeur automatique
- Vers
- Objet de l'assistant du navigateur
- URL d'hameçonnage
- Logiciels publicitaires
- Fichier chiffré
- Impossible à analyser
- Autres programmes malveillants

Analyse Webroot

Le moteur d'analyse Webroot inspecte les objets pour déterminer le verdict de l'analyse des programmes malveillants à envoyer au moteur DVS. Le moteur d'analyse Webroot inspecte les objets suivants :

- **Demande d'URL.** Webroot évalue une demande d'URL pour déterminer si l'URL pourrait être malveillante. Si Webroot soupçonne que la réponse à partir de cette URL peut contenir un programme malveillant, l'appliance surveille ou bloque la demande, selon la configuration de l'appliance. Si l'évaluation Webroot efface la demande, l'appliance récupère l'URL et analyse la réponse du serveur.
- **Réponse du serveur.** Lorsque l'appliance récupère une URL, Webroot analyse le contenu de la réponse du serveur et le compare à la base de données de signatures Webroot.

Analyse McAfee

Le moteur d'analyse McAfee inspecte les objets téléchargés à partir d'un serveur Web dans les réponses HTTP. Après avoir inspecté l'objet, il transmet un verdict d'analyse de programmes malveillants au moteur DVS pour que ce dernier puisse déterminer s'il faut surveiller ou bloquer la demande.

Le moteur d'analyse McAfee utilise les méthodes suivantes pour déterminer le verdict de l'analyse contre les programmes malveillants :

- Correspondance des schémas de signature de virus
- Analyse heuristique

Correspondance des schémas de signature de virus

McAfee utilise les définitions de virus dans sa base de données avec son moteur d'analyse pour détecter des virus, des types de virus ou d'autres logiciels potentiellement indésirables. Il recherche les signatures de virus dans les fichiers. Lorsque vous activez McAfee, le moteur d'analyse McAfee utilise cette méthode pour analyser le contenu de la réponse du serveur.

Analyse heuristique

L'analyse heuristique est une technique qui utilise des règles générales plutôt que des règles spécifiques pour détecter les nouveaux virus et programmes malveillants. Lorsque le moteur d'analyse McAfee utilise l'analyse

heuristique, il examine le code d'un objet, applique des règles génériques et détermine la probabilité que l'objet ressemble à un virus.

L'utilisation de l'analyse heuristique augmente le risque de signalement de faux positifs (contenu sain désigné comme virus) et pourrait avoir un impact sur les performances de l'appliance. Lorsque vous activez McAfee, vous pouvez choisir d'activer ou non l'analyse heuristique lors de l'analyse d'objets.

Catégories McAfee

Verdit McAfee	Catégorie du verdict de l'analyse contre les programmes malveillants
Virus connus	Virus
Cheval de Troie	Cheval de Troie
Fichier de recommandation	Logiciels publicitaires
Fichier de test	Virus
Candidats	Virus
Tué	Virus
Application commerciale	Supervision de système commercial
Objet potentiellement indésirable	Logiciels publicitaires
Progiciel potentiellement indésirable	Logiciels publicitaires
Fichier chiffré	Fichier chiffré

Analyse Sophos

Le moteur d'analyse Sophos inspecte les objets téléchargés à partir d'un serveur Web dans les réponses HTTP. Après avoir inspecté l'objet, il transmet un verdict d'analyse de programmes malveillants au moteur DVS pour que ce dernier puisse déterminer s'il faut surveiller ou bloquer la demande. Vous pourriez souhaiter activer le moteur d'analyse Sophos au lieu du moteur d'analyse McAfee si le logiciel antiprogramme malveillant McAfee est installé.

Interprétation de l'analyse adaptative

L'analyse adaptative décide quel moteur d'analyse de protection contre les programmes malveillants (y compris l'analyse Cisco Secure Endpoint pour les fichiers téléchargés) traitera la demande Web.

L'analyse adaptative applique la catégorie de programmes malveillants « Outbreak Heuristics » aux transactions qu'elle considère comme des programmes malveillants avant d'exécuter un moteur d'analyse. Vous pouvez choisir de bloquer ou non ces transactions lorsque vous configurez les paramètres de la protection contre les programmes malveillants sur l'appliance.

Analyse adaptative et politiques d'accès

Lorsque l'analyse adaptative est activée, certains paramètres de protection contre les programmes malveillants et de réputation que vous pouvez configurer dans les politiques d'accès sont légèrement différents :

- Vous pouvez activer ou désactiver le filtrage de réputation de sites Web dans chaque politique d'accès, mais vous ne pouvez pas modifier les scores de réputation Web.
- Vous pouvez activer l'analyse de protection contre les programmes malveillants dans chaque politique d'accès, mais vous ne pouvez pas choisir le moteur d'analyse de protection contre les programmes malveillants à activer. L'analyse adaptative choisit le moteur le plus approprié pour chaque demande Web.

Note Si l'analyse adaptative n'est pas activée et que des paramètres de réputation Web et de protection contre les programmes malveillants particuliers sont configurés pour une politique d'accès, tous les paramètres de réputation Web et de protection contre les programmes malveillants existants sont alors remplacés.

Les paramètres Cisco Secure Endpoint de chaque politique sont les mêmes, que l'analyse adaptative soit activée ou non.

Activation des filtres contre les programmes malveillants et de réputation

Before you begin

Vérifiez que les filtres de réputation des sites Web, le moteur DVS et les moteurs d'analyse Webroot, McAfee et Sophos sont activés. Par défaut, ils doivent être activés lors de la configuration du système.

Étape 1 Choisissez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants réputation).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Configurez les paramètres selon vos besoins.

Paramètres	Description
Filtrage de réputation Web	Choisissez d'activer ou non le filtrage de réputation Web.
Analyse adaptative	Choisissez d'activer ou non l'analyse adaptative. Vous pouvez uniquement activer l'analyse adaptative lorsque le filtrage de réputation Web est activé.
Filtrage de réputation de fichiers et analyse de fichiers	Voir Activation et configuration des services de réputation et d'analyse des fichiers .

Paramètres	Description
Intégration de la console Cisco Secure Endpoint [**Advanced** > **Advanced Settings for File Reputation** (Avancé > Paramètres avancés pour la réputation des fichiers)]	Cliquez sur **Register the Appliance with** Secure Endpoint to integrate your appliance with Secure Endpoint (Enregistrer l'appliance auprès de Cisco Secure Endpoint AMP for Endpoints) pour intégrer votre appliance à la console Cisco Secure Endpoint AMP for Endpoints). Pour plus d'informations sur les instructions, consultez Intégration de l'appliance à la console Secure Endpoint AMP for Endpoints, on page 317.
Limites d'analyse des objets du moteur DVS	Indiquez une pour l'analyse. La valeur de la taille maximale de l'objet que vous spécifiez s'applique à la taille complète des demandes et des réponses qui peuvent être analysées par tous les moteurs d'analyse de programmes malveillants et de virus et parCisco Secure Endpoint les fonctionnalités. Elle indique également la taille maximale d'une archive pouvant être inspectée pour l'inspection des archives; voir Politiques d'accès : blocage d'objets, on page 262 pour en savoir plus sur l'inspection des archives. Lorsqu'une taille de chargement ou de téléchargement dépasse cette taille, le composant de sécurité peut interrompre l'analyse en cours et peut ne pas fournir de verdict d'analyse au proxy Web. Si une archive pouvant être inspectée dépasse cette taille, elle est marquée « Not Scanned » (Non analysée).
Sophos	Choisissez d'activer ou non le moteur d'analyse Sophos.
McAfee	Choisissez d'activer ou non le moteur d'analyse McAfee. Lorsque vous activez le moteur d'analyse McAfee, vous pouvez choisir d'activer ou non l'analyse heuristique. **Note** L'analyse heuristique augmente la protection de la sécurité, mais peut entraîner de faux positifs et réduire les performances.
Webroot	Choisissez d'activer ou non le moteur d'analyse Webroot. Lorsque vous activez le moteur d'analyse Webroot, vous pouvez configurer le seuil de risque pour les menaces (TRT). Le seuil de risque pour les menaces attribue une valeur numérique à la probabilité que des programmes malveillants existent. Des algorithmes exclusifs évaluent le résultat d'une séquence de correspondance d'URL et attribuent une évaluation de risque de menace (TRR). Cette valeur est associée au paramètre de seuil de menace. Si la valeur TRR est supérieure ou égale à la valeur TRT, l'URL est considérée comme un programme malveillant et est transmise pour traitement ultérieur. **Note** La définition du seuil de risque de menace sur une valeur inférieure à 90 augmente considérablement le taux de blocage d'URL et rejette les demandes légitimes. Cisco recommande fortement de maintenir la valeur par défaut du TRT à 90. La valeur minimale d'un paramètre TRT est 51.

Étape 4 Envoyez et validez les modifications.

What to do next

- Interprétation de l'analyse adaptative, on page 309
- Analyse McAfee, on page 308

Effacement du cache des services Cisco Secure Endpoint

La fonctionnalité d'effacement du cache Cisco Secure Endpoint efface les dispositions de réputation des fichiers sains, malveillants et inconnus.

Remarque Le cache Cisco Secure Endpoint est utilisé pour augmenter les performances. En utilisant la commande **Clear Cache** (Effacer le cache), vous pourriez observer une dégradation temporaire des performances pendant le remplissage du cache.

Étape 1 Choisissez **Security Services** > **Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation).

Étape 2 Dans la section Cisco Secure Endpoint Services, cliquez sur **Clear Cache** (Effacer le cache) et confirmez votre action.

Configuration des politiques de protection contre les programmes malveillants et de réputation

Lorsque les filtres de protection contre les programmes malveillants et de réputation sont activés sur l'appliance, vous pouvez configurer différents paramètres dans les groupes de politiques. Vous pouvez activer la supervision ou le blocage des catégories de programmes malveillants en fonction des verdicts de l'analyse des programmes malveillants.

Vous pouvez configurer les paramètres de la protection contre les programmes malveillants dans les groupes de politiques suivants :

Type de politique	Lien vers la tâche
Politiques d'accès	Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès, on page 313
Politiques d'analyse des programmes malveillants sortants	Contrôle des demandes de téléchargement à l'aide des politiques d'analyse des programmes malveillants sortants

Vous pouvez configurer les paramètres de réputation Web dans les groupes de politiques suivants :

Type de politique	Lien vers la tâche
Politiques d'accès	Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès, on page 313
Politiques de déchiffrement	Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement, on page 316

Type de politique	Lien vers la tâche
Politiques de sécurité des données de Cisco	Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement, on page 316

Vous pouvez configurer les paramètres Cisco Secure Endpoint uniquement dans les politiques d'accès. Voir la section Configuration des fonctionnalités d'analyse et de réputation de fichiers, on page 328.

Paramètres de protection contre les programmes malveillants et de réputation dans les politiques d'accès

Lorsque l'analyse adaptative est activée, les paramètres de réputation Web et de protection contre les programmes malveillants que vous pouvez configurer pour les politiques d'accès sont légèrement différents de ceux que vous pouvez définir lorsque l'analyse adaptative est désactivée.

Note Si votre déploiement comprend une appliance de gestion de la sécurité et que vous configurez cette fonctionnalité dans un fichier de configuration principal, les options disponibles dans cette page dépendent de l'activation de la sécurité adaptative pour la configuration principale concernée ou non. Vérifiez le paramètre sur l'appliance de gestion de la sécurité, sur la page **Web > Utilities > Security Services Display** (Web > Utilitaires > Affichage des services de sécurité).

- Interprétation de l'analyse adaptative, on page 309

Configuration des paramètres de protection contre les programmes malveillants et de réputation avec l'analyse adaptative activée

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien **Anti-Malware and Reputation** (Antiprogrammes malveillants et réputation) pour la politique d'accès que vous souhaitez configurer.

Étape 3 Dans la section **Web Reputation and Anti-Malware Settings** (Paramètres de réputation Web et de protection contre les programmes malveillants), choisissez **Define Web Reputation and Anti-Malware Custom Settings** (Définir les paramètres personnalisés de réputation Web et de protection contre les programmes malveillants).

Cela vous permet de configurer les paramètres de réputation Web et de protection contre les programmes malveillants pour cette politique d'accès qui sont différents de la politique globale.

Étape 4 Dans la section **Web Reputation Settings** (Paramètres de réputation Web), choisissez d'activer ou non le filtrage de réputation Web. L'analyse adaptative choisit les seuils de score de réputation Web les plus appropriés pour chaque demande Web.

Étape 5 Configurez les paramètres dans la section Cisco Secure Endpoint **Settings** (Paramètres).

Étape 6 Faites défiler la liste jusqu'à la section des paramètres de Cisco DVS Anti-Malware.

Étape 7 Configurez les paramètres de protection contre les programmes malveillants pour la politique au besoin.

Activer l'analyse des agents utilisateur suspects	Choisissez si vous souhaitez analyser ou non le trafic en fonction du champ user-agent spécifié dans l'en-tête de la demande HTTP. Lorsque vous cochez cette case, vous pouvez choisir de surveiller ou de bloquer les agents utilisateur suspects dans la section Additional Scanning (Analyse supplémentaire) au bas de la page. **Note** Les navigateurs Chrome n'incluent pas de chaîne user-agent dans les demandes FTP-sur-HTTP ; par conséquent, Chrome ne peut pas être détecté en tant qu'agent utilisateur dans ces demandes.
Activer l'analyse des programmes malveillants	Choisissez si vous souhaitez utiliser ou non le moteur DVS pour analyser le trafic à la recherche de programmes malveillants. L'analyse adaptative choisit le moteur le plus approprié pour chaque demande Web.
Malware Categories (Catégorie de programmes malveillants)	Choisissez de surveiller ou de bloquer les différentes catégories de programmes malveillants en fonction du verdict de l'analyse.
Autres catégories	Choisissez si vous souhaitez surveiller ou bloquer les types d'objets et les réponses répertoriés dans cette section. **Note** La catégorie Outbreak Heuristics (Heuristique des épidémies) s'applique aux transactions identifiées comme malveillantes par l'analyse adaptative avant l'exécution de tout moteur d'analyse. **Note** Les transactions URL sont classées comme non analysables lorsque le paramètre de durée maximale configuré est atteint ou lorsque le système éprouve une condition d'erreur transitoire. Par exemple, les transactions peuvent être classées comme non analysables lors des mises à jour du moteur d'analyse ou des mises à niveau d'AsyncOS. Les verdicts d'analyse des programmes malveillants SV_TIMEOUT et SV_ERROR sont considérés comme des transactions non analysables.

Étape 8 Envoyez et validez les modifications.

What to do next

- Interprétation de l'analyse adaptative, on page 309

Configuration des paramètres de protection contre les programmes malveillants et de réputation avec l'analyse adaptative désactivée

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien **Anti-Malware and Reputation** (Antiprogrammes malveillants et réputation) pour la politique d'accès que vous souhaitez configurer.

Étape 3 Dans la section **Web Reputation and Anti-Malware Settings** (Paramètres de réputation Web et de protection contre les programmes malveillants), choisissez **Define Web Reputation and Anti-Malware Custom Settings** (Définir les paramètres personnalisés de réputation Web et de protection contre les programmes malveillants).

Cela vous permet de configurer les paramètres de réputation Web et de protection contre les programmes malveillants pour cette politique d'accès qui sont différents de la politique globale.

Étape 4 Configurez les paramètres dans la section **Web Reputation Settings** (Paramètres de réputation Web).

Étape 5 Configurez les paramètres dans la section Cisco Secure Endpoint **Settings** (Paramètres).

Étape 6 Faites défiler la liste jusqu'à la section des paramètres de Cisco DVS Anti-Malware.

Étape 7 Configurez les paramètres de protection contre les programmes malveillants pour la politique au besoin.

Note Lorsque vous activez le contrôle Webroot, Sophos ou McAfee, vous pouvez choisir de surveiller ou de bloquer certaines catégories supplémentaires dans les catégories de programmes malveillants sur cette page.

Paramètres	Description
Activer l'analyse des agents utilisateur suspects	Choisissez d'activer ou non l'appliance pour analyser le trafic en fonction du champ user-agent spécifié dans l'en-tête de la demande HTTP. Lorsque vous cochez cette case, vous pouvez choisir de surveiller ou de bloquer les agents utilisateur suspects dans la section Additional Scanning (Analyse supplémentaire) au bas de la page. **Note** Les navigateurs Chrome n'incluent pas de chaîne user-agent dans les demandes FTP-sur-HTTP ; par conséquent, Chrome ne peut pas être détecté en tant qu'agent utilisateur dans ces demandes.
Activer Webroot	Choisissez si vous souhaitez permettre à l'appliance d'utiliser le moteur d'analyse Webroot lors de l'analyse du trafic.
Activer Sophos ou McAfee	Choisissez d'activer ou non l'appliance pour utiliser le moteur d'analyse Sophos ou McAfee lors de l'analyse du trafic.
Malware Categories (Catégorie de programmes malveillants)	Choisissez de surveiller ou de bloquer les différentes catégories de programmes malveillants en fonction du verdict de l'analyse. Les catégories répertoriées dans cette section dépendent des moteurs d'analyse que vous avez activés ci-dessus.
Autres catégories	Choisissez si vous souhaitez surveiller ou bloquer les types d'objets et les réponses répertoriés dans cette section. **Note** Les transactions URL sont classées comme non analysables lorsque le paramètre de durée maximale configuré est atteint ou lorsque le système éprouve une condition d'erreur transitoire. Par exemple, les transactions peuvent être classées comme non analysables lors des mises à jour du moteur d'analyse ou des mises à niveau d'AsyncOS. Les verdicts d'analyse des programmes malveillants SV_TIMEOUT et SV_ERROR sont considérés comme des transactions non analysables.

Étape 8 Envoyez et validez les modifications.

What to do next

- Configuration des seuils de score de réputation Web pour les politiques d'accès, on page 316

• Descriptions des catégories de programmes malveillants, on page 321

Configuration des scores de réputation Web

Lorsque vous installez et configurez Secure Web Appliance, les paramètres par défaut pour les scores de réputation de sites Web sont appliqués. Toutefois, vous pouvez modifier les paramètres de seuil pour l'évaluation de la réputation Web selon les besoins de votre organisation. Vous configurez les paramètres de filtre de réputation Web pour chaque groupe de politiques.

Configuration des seuils de score de réputation Web pour les politiques d'accès

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien sous la colonne **Anti-Malware and Reputation** (Protection contre les programmes malveillants et réputation) du groupe de politiques d'accès que vous souhaitez modifier.

Étape 3 Dans la section **Web Reputation and Anti-Malware Settings** (Paramètres de réputation Web et de protection contre les programmes malveillants), choisissez **Define Web Reputation and Anti-Malware Custom Settings** (Définir les paramètres personnalisés de réputation Web et de protection contre les programmes malveillants).

Cela vous permet de configurer les paramètres de réputation Web et de protection contre les programmes malveillants pour cette politique d'accès qui sont différents de la politique globale.

Étape 4 Vérifiez que le champ **Enable Web Reputation Filtering** (Activer le filtrage de réputation Web) est activé.

Étape 5 Déplacez les marqueurs pour modifier la plage des actions de blocage, d'analyse et d'autorisation d'URL.

Étape 6 Envoyez et validez les modifications.

Note Vous pouvez modifier les seuils de score de réputation Web dans les politiques d'accès lorsque l'analyse adaptative est désactivée.

Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement

Étape 1 Choisissez **Web Security Manager > Decryption Policies** (Web Security Manager > Politiques de déchiffrement).

Étape 2 Cliquez sur le lien sous la colonne Web Reputation (Réputation Web) pour le groupe de politiques de déchiffrement que vous souhaitez modifier.

Étape 3 Dans la section **Web Reputation Settings** (Paramètres de réputation Web), choisissez **Define Web Reputation Custom Settings** (Définir les paramètres personnalisés de réputation Web). Cela vous permet de remplacer les paramètres de réputation Web du groupe de politiques globales.

Étape 4 Vérifiez que le champ **Enable Web Reputation Filtering** (Activer le filtrage de réputation Web) est coché.

Étape 5 Déplacez les repères pour modifier la plage des actions de suppression, de déchiffrement et de transmission d'URL.

Étape 6 Dans le champ **Sites with No Score** (Sites sans score de réputation), choisissez l'action à entreprendre sur la demande pour les sites auxquels aucun score de réputation Web n'est affecté.

Étape 7 Envoyez et validez les modifications.

Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de sécurité des données

Étape 1 Choisissez **Web Security Manager > Cisco Data Security** (Web Security Manager > Politiques de sécurité des données de Cisco).

Étape 2 Cliquez sur le lien sous la colonne de réputation Web pour le groupe de politiques de sécurité des données que vous souhaitez modifier.

Étape 3 Dans la section **Web Reputation Settings** (Paramètres de réputation Web), choisissez **Define Web Reputation Custom Settings** (Définir les paramètres personnalisés de réputation Web).

Cela vous permet de remplacer les paramètres de réputation Web du groupe de politiques globales.

Étape 4 Déplacez le marqueur pour modifier la plage de blocage d'URL et surveiller les actions.

Étape 5 Envoyez et validez les modifications.

Note Seules des valeurs négatives et nulles peuvent être configurées pour les paramètres de seuil de réputation de sites Web pour les politiques de sécurité des données de Cisco. Par définition, toutes les évaluations positives sont surveillées

Intégration de l'appliance à la console Secure Endpoint AMP for Endpoints

Vous pouvez intégrer votre appliance à la console Secure Endpoint et effectuer les actions suivantes dans la console de Secure Endpoint :

- Créez une liste de détection personnalisée simple.
- Ajoutez de nouvelles informations SHA de fichiers malveillants à la liste de détection personnalisée simple.
- Créez une liste des applications autorisées.
- Ajoutez de nouvelles informations SHA de fichiers à la liste des applications autorisées.
- Créez une politique personnalisée.
- Associez la liste de détection personnalisée simple et la liste des applications autorisées à la politique personnalisée.
- Créez un groupe personnalisé.
- Associez la politique personnalisée au groupe personnalisé.
- Déplacez votre appliance enregistrée du groupe par défaut vers le groupe personnalisé.
- Affichez les détails de la trajectoire de fichier des informations SHA d'un fichier particulier.

Pour intégrer votre appliance à la console Secure Endpoint, vous devez enregistrer votre appliance auprès de la console.

Après l'intégration, quand les informations SHA du fichier sont envoyées au serveur de réputation des fichiers, le verdict obtenu pour les informations SHA du fichier à partir du serveur de réputation des fichiers est remplacé par le verdict déjà disponible pour les mêmes informations SHA du fichier dans la console Cisco Secure Endpoint.

Si un fichier SHA est déjà marqué comme malveillant dans le monde et si le même SHA de fichier est ajouté à la liste de blocage dans la console Secure Endpoint, la disposition du fichier est malveillante.

La page de rapport Cisco Secure Endpoint comprend une nouvelle section **Incoming Malware Files by Category** (Fichiers malveillants entrants par catégorie) pour afficher le pourcentage d'informations SHA du fichier de la liste de blocage reçues de la console Secure Endpoint qui sont affichés comme **Custom Detection** (Détection personnalisée). Le nom de menace d'informations SHA du fichier de la liste de blocage est affiché comme **Simple Custom Detection** (Détection personnalisée simple) dans la section des fichiers de programmes malveillants entrants du rapport. Vous pouvez cliquer sur le lien dans la section More Details (Plus de détails) du rapport pour afficher les détails de la trajectoire des informations SHA d'un fichier de la liste de blocage dans la console Secure Endpoint.

La page de rapport Cisco Secure Endpoint comprend une nouvelle section **Incoming Malicious Files by Category** (Fichiers malveillants entrants par catégorie) pour afficher le pourcentage d'informations SHA du fichier de la liste de blocage reçues de la console de la console Secure Endpoint qui sont affichées comme **Custom Detection** (Détection personnalisée). Le nom de menace des informations SHA d'un fichier de la liste de blocage s'affiche comme **Détection personnalisée** dans la section Malicious Threat Files (Fichiers de programmes malveillants) du rapport. Pour afficher les détails de la trajectoire des informations SHA d'un fichier de la liste de blocage dans la console Secure Endpoint, consultez #unique_459.

Avant de commencer

Assurez-vous d'avoir un compte d'utilisateur dans la console Cisco Secure Endpoint avec des droits d'accès admin. Pour en savoir plus sur la création d'un compte d'utilisateur sur la console Cisco Secure Endpoint, communiquez avec le service d'assistance technique de Cisco.

[Pour une configuration en grappe] Dans une configuration en grappe, vous pouvez uniquement enregistrer l'appliance connectée auprès de la console Secure Endpoint. Si vous avez déjà enregistré votre appliance auprès de la console Secure Endpoint en mode autonome, veillez à annuler l'enregistrement de l'appliance manuellement avant de l'associer à une grappe.

Assurez-vous d'avoir activé et configuré le filtrage de réputation des fichiers. Consultez la section Activation et configuration des services de réputation et d'analyse des fichiers pour savoir comment activer et configurer le filtrage de réputation des fichiers.

Étape 1 Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cliquez sur **Register Appliance with** Secure Endpoint (Enregistrer l'appliance auprès de Secure Endpoint) pour obtenir la réputation du fichier dans la page File Reputation and File Analysis (Réputation des fichiers et analyse des fichiers) de l'interface Web.

Lorsque vous avez cliqué sur Register Appliance with Secure Endpoint (Enregistrer l'appliance auprès de Secure Endpoint), la page de connexion de la console Secure Endpoint s'affiche.

Étape 4 Cliquez sur **Register Appliance with** Secure Endpoint (Enregistrer l'appliance auprès de Cisco Secure Endpoint) dans le volet Advanced Settings (Paramètres avancés) pour la réputation des fichiers sur la page Anti-Malware and Reputation (Protection contre les programmes malveillants et réputation) de l'interface Web.

Lorsque vous avez cliqué sur Register Appliance with Secure Endpoint (Enregistrer l'appliance auprès de Secure Endpoint), la page de connexion de la console Secure Endpoint s'affiche.

Remarque Vous devez activer et configurer le filtrage de réputation de fichiers avant d'enregistrer l'appliance auprès de Secure Endpoint. Consultez la section sur l'Activation et configuration des services de réputation et d'analyse des fichiers pour savoir comment activer et configurer le filtrage de réputation des fichiers.

Étape 5 Connectez-vous à la console Cisco Secure Endpoint avec vos informations d'identification utilisateur.

Étape 6 Cliquez sur **Allow** (Autoriser) dans la page d'autorisation de Secure Endpoint pour enregistrer votre appliance.

Une fois que vous avez cliqué sur Allow (Autoriser), l'enregistrement est terminé et vous êtes redirigé vers la page de réputation de la protection contre les programmes malveillants de votre appliance. Le nom de votre appliance s'affiche dans le champ d'intégration de la console Cisco Secure Endpoint. Vous pouvez utiliser le nom de l'appliance pour personnaliser les paramètres de votre appliance dans la page de la console Secure Endpoint.

Prochaine étape

Prochaines étapes :

- Vous pouvez accéder à la section Accounts > Applications (Comptes > Applications) de la page de la console Cisco Secure Endpoint afin de vérifier si votre appliance est enregistrée auprès de la console Cisco Secure Endpoint. Le nom de votre appliance s'affiche dans la section Applications de la page de la console Cisco Secure Endpoint.
- Après l'enregistrement, votre appliance est ajouté au groupe par défaut (Groupe d'audit) auquel une politique par défaut (Politique réseau) est attachée. La politique par défaut contient les informations SHA du fichier qui sont ajoutées à la liste de blocage ou à la liste des autorisations. Si vous souhaitez personnaliser les paramètres de Cisco Secure Endpoint pour votre appliance et ajouter vos propres informations SHA du fichier qui sont ajoutées à la liste des blocages ou à la liste des autorisations, consultez la documentation de l'utilisateur Cisco Secure Endpoint dans https://console.amp.cisco.com/docs.
- Pour annuler l'enregistrement de la connexion de votre appliance auprès de la console Cisco Secure Endpoint, vous pouvez cliquer sur **Deregister** (Annuler l'enregistrement) dans la section Advanced Settings for File Reputation (Paramètres avancés de réputation des fichiers) de votre appliance ou vous devez vous rendre à la page de la console Cisco Secure Endpoint à l'adresse https://console.amp.cisco.com/ . Pour en savoir plus, consultez la documentation utilisateur de Secure Endpoint à l'adresse https://console.amp.cisco.com/docs.

Remarque Lorsque vous changez votre serveur de réputation des fichiers dans un autre centre de données, l'enregistrement de votre appliance est automatiquement annulé dans la console Secure Endpoint. Vous devez réenregistrer votre appliance auprès de la console Secure Endpoint avec le même centre de données que celui qui a été sélectionné pour le serveur de réputation des fichiers.

Remarque Si les informations SHA d'un fichier malveillant obtient un verdict sain, vérifiez si les mêmes informations SHA du fichier sont ajouté à la liste des autorisations dans la console Secure Endpoint.

Gestion des tableaux de base de données

Les bases de données de réputation de sites Web, Webroot, Sophos et McAfee reçoivent régulièrement des mises à jour du serveur de mise à jour Cisco. Les mises à jour du serveur sont automatisées et l'intervalle des mises à jour est défini par le serveur.

Base de données sur la réputation Web

Secure Web Appliance gère une base de données de filtrage qui contient des statistiques et des renseignements sur le traitement des différents types de demandes. L'appliance peut également être configurée pour envoyer des statistiques de réputation Web à un serveur du réseau Cisco SensorBase. Les informations du serveur SensorBase sont exploitées avec des flux de données du réseau SensorBase et les informations sont utilisées pour produire un score de réputation Web.

Journalisation de l'activité de filtrage de la réputation Web et de l'analyse DVS

Le fichier journal des accès enregistre les informations renvoyées par les filtres de réputation Web et le moteur DVS pour chaque transaction. La section des renseignements sur le verdict d'analyse dans les journaux d'accès comprend de nombreux champs pour aider à comprendre la cause de l'action appliquée à une transaction. Par exemple, certains champs affichent le score de réputation Web ou le verdict de recherche de programmes malveillants transmis par Sophos au moteur DVS.

Journalisation de l'analyse adaptative

Champ personnalisé dans les journaux d'accès	Champ personnalisé dans les journaux W3C	Description
%X6	x-as-malware-threat-name	Le nom de la solution antiprogramme malveillant renvoyé par l'analyse adaptative. Si la transaction n'est pas bloquée, ce champ renvoie un tiret (« - »). Cette variable est incluse dans les informations sur le verdict de l'analyse (entre les crochets à la fin de chaque entrée du journal des accès).

Les transactions bloquées et surveillées par le moteur d'analyse adaptative utilisent les balises de décision d'ACL :

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

Caching (Mise en mémoire cache)

Les directives suivantes expliquent comment AsyncOS utilise le cache lors de la recherche de programmes malveillants :

- AsyncOS ne met en cache les objets que si l'objet entier est téléchargé. Si le programme malveillant est bloqué pendant l'analyse, l'objet entier n'est pas téléchargé et, par conséquent, n'est pas mis en cache.
- AsyncOS analyse le contenu, qu'il soit récupéré depuis le serveur ou le cache Web.
- La durée pendant laquelle le contenu est mis en cache varie en fonction de nombreux facteurs. Il n'y a pas de valeur par défaut.
- AsyncOS analyse de nouveau le contenu lorsque les signatures sont mises à jour.

Descriptions des catégories de programmes malveillants

Type de maliciel	Description
Logiciels publicitaires	Les logiciels publicitaires englobent tous les exécutables logiciels et les modules d'extension qui dirigent les utilisateurs vers les produits à vendre. Ces programmes peuvent également modifier les paramètres de sécurité, en empêchant les utilisateurs de modifier les paramètres système.
Objet de l'assistant du navigateur	Un objet assistant de navigateur est un module d'extension de navigateur qui peut remplir diverses fonctions liées à la diffusion de publicités ou au détournement de paramètres utilisateur.
Supervision de système commercial	Un moniteur système commercial est un logiciel ayant les caractéristiques d'un moniteur système qui peut être obtenu avec une licence légitime par des moyens légaux.
Composeur automatique	Un composeur est un programme qui utilise votre modem ou un autre type d'accès Internet pour vous connecter à une ligne téléphonique ou à un site qui vous fait accumuler des frais d'interurbain pour lesquels vous n'avez pas donné votre plein consentement.
Logiciel espion générique	Un logiciel espion est un type de programme malveillant installé sur les ordinateurs qui recueille de petits éléments d'information sur les utilisateurs à l'insu des utilisateurs.
Détournement d'identité	Un pirate modifie les paramètres système ou toutes les modifications indésirables apportées au système d'un utilisateur qui peut le diriger vers un site Web ou exécuter un programme sans le consentement de l'utilisateur.
Fichiers malveillants ou à risque élevé connus	Il s'agit de fichiers qui ont été identifiés comme des menaces par le service de réputation de fichiers Cisco Secure Endpoint.
Autres programmes malveillants	Cette catégorie est utilisée pour détecter tous les autres programmes malveillants et comportements suspects qui n'entrent pas exactement dans l'une des autres catégories définies.

Type de maliciel	Description
URL d'hameçonnage	Une URL d'hameçonnage s'affiche dans la barre d'adresse du navigateur. Dans certains cas, elle implique l'utilisation de noms de domaine et ressemble à celle de domaines légitimes.
API (applications potentiellement indésirables)	Application potentiellement indésirable. Un PUA est une application qui n'est pas malveillante, mais qui peut être considérée comme indésirable.
Moniteur système	Un moniteur système englobe tout logiciel qui effectue l'une des opérations suivantes : • Enregistre ouvertement ou secrètement les processus du système et/ou les actions de l'utilisateur; • Rend ces enregistrements disponibles pour la récupération et l'examen ultérieurement.
Outil de téléchargement de chevaux de Troie	Un logiciel de téléchargement de chevaux de Troie désigne un cheval de Troie qui, après son installation, communique avec un hôte ou un site distant et installe des paquets ou des sociétés affiliées à partir de l'hôte distant.
Cheval de Troie	Un cheval de Troie est un programme destructeur qui se fait passer pour une application inoffensive. Contrairement aux virus, les chevaux de Troie ne se reproduisent pas.
Cheval de Troie pour hameçonnage	Un cheval de Troie pour hameçonnage peut rester sur un ordinateur infecté en attendant la visite d'une page Web spécifique ou peut analyser l'ordinateur infecté à la recherche de noms d'utilisateur et de phrases secrètes.
Virus	Un virus est un programme ou un élément de code qui est chargé sur votre ordinateur à votre insu.
Vers	Un ver est un programme ou un algorithme qui se reproduit sur un réseau informatique et qui effectue des actions malveillantes.

CHAPITRE 14

Filtrage de réputation de fichiers et analyse de fichiers

Le présent chapitre contient les sections suivantes :

Survol du filtrage de réputation de fichiers et de l'analyse de fichiers

Cisco Secure Endpoint assure une protection contre les menaces de type « zero day » et basées sur un fichier cibleen :

- obtenant la réputation des fichiers connus ;
- analysant le comportement de certains fichiers qui ne sont pas encore connus du service de réputation ;
- évaluant en permanence les menaces émergentes au fur et à mesure que de nouvelles informations sont disponibles et en vous informant des fichiers qui sont considérés comme des menaces après leur entrée dans votre réseau.

Cette fonction est disponible pour les téléchargements de fichiers. Fichiers chargés.

Les services de réputation de fichier et d'analyse de fichier proposent des options pour un cloud public ou privé (sur site).

- Le service de réputation de fichier de cloud privé est fourni par l'appliance Cisco Virtual Private Cloud, fonctionnant en mode Cisco Secure Endpoint « proxy » ou « air-gap » (sur site). Consultez Configuration d'un serveur de réputation de fichiers sur site, on page 331.
- Le service d'analyse des fichiers de cloud privé est fourni par une appliance Cisco Cisco Secure Endpoint Malware Analytics sur site. Consultez Configuration d'un serveur d'analyse de fichiers sur site , on page 331.

Mises à jour des verdicts de menaces des fichiers

Les verdicts de menaces peuvent changer à mesure que de nouvelles informations sont disponibles. Un fichier peut initialement être évalué comme inconnu ou sain et l'utilisateur peut ainsi être autorisé à y accéder;. Si le verdict de menace change à mesure que de nouveaux renseignements sont disponibles, vous en serez alerté, et le fichier et son nouveau verdict s'afficheront dans le rapport sur les mises à jour des verdicts Cisco Secure Endpoint . Vous pouvez examiner la du message au point d'entrée comme point de départ pour remédier aux éventuels impacts de la menace.

Les verdicts peuvent également passer de malveillants à sains.

Lorsque l'appliance traite les instances suivantes du même fichier, le verdict mis à jour est immédiatement appliqué.

Des renseignements sur le moment des mises à jour des verdicts sont inclus dans le document sur les critères de fichier mentionné dans Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 326.

Thèmes connexes

- Création de rapports et suivi de la réputation et de l'analyse des fichiers , on page 340
- Mesures à prendre lors de changements de verdicts des menaces de fichiers , on page 344

Survol du traitement de fichiers

Tout d'abord, le site Web à partir duquel le fichier est téléchargé est évalué en fonction du service de réputation Web (WBRS).

Si le score de réputation Web du site se trouve dans la plage configurée pour « Scan » (Analyse), l'appliance analyse simultanément la transaction à la recherche de programmes malveillants et interroge le service en nuage sur la réputation du fichier. (Si le score de réputation du site se situe dans la plage « Block », la transaction est gérée en conséquence et il n'est pas nécessaire de traiter le fichier davantage.) Si un programme malveillant est détecté lors de l'analyse, la transaction est bloquée, quelle que soit la réputation du fichier.

Si l'analyse adaptative est également activée, l'évaluation de la réputation des fichiers et l'analyse des fichiers sont incluses dans l'analyse adaptative.

Les communications entre l'appliance et le service de réputation des fichiers sont chiffrées et protégées contre la falsification.

Après l'évaluation de la réputation d'un fichier :

- Si le fichier est connu du service de réputation de fichiers et qu'il est déterminé comme étant sain, il est remis à l'utilisateur final et .
- Si le service de réputation des fichiers renvoie un verdict malveillant l'appliance applique l'action que vous avez spécifiée à ces fichiers.
- Si le fichier est connu du service de réputation, mais qu'il n'y a pas suffisamment d'informations pour un verdict définitif, le service de de menace en fonction des caractéristiques du fichier telles que l'analyse de l'empreinte de la menace et du comportement. Si ce score atteint ou dépasse le seuil de réputation configuré, l'appliance applique l'action que vous avez configurée dans la politique d'accès de pour les malveillants ou des fichiers à risque élevé.
- Si le service de réputation ne possède aucune information à propos du fichier et que le fichier ne répond pas aux critères d'analyse (voir Fichiers pris en charge pour les services de réputation et d'analyse des

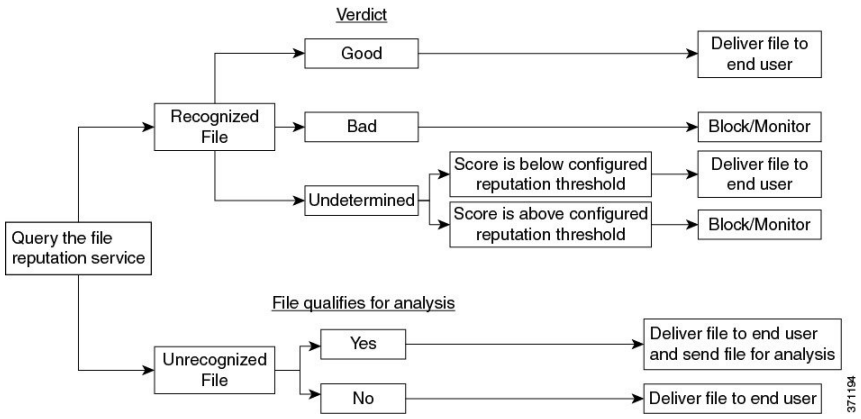
fichiers , on page 326), le fichier est considéré comme non sain et il est mis à la disposition de l'utilisateur final .

- Si vous avez activé le service d'analyse de Fichiers en nuage et que le service de réputation ne possède aucune information à propos du fichier et que le fichier répond aux critères des fichiers pouvant être analysés (voir Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 326), le fichier est considéré comme sain et est facultativement pour analyse.
- Pour les déploiements avec analyse de fichiers sur site, l'évaluation de la réputation et l'analyse de fichier ont lieu simultanément. Si le service de réputation renvoie un verdict, ce verdict est utilisé, car le service de réputation comprend des entrées provenant d'un éventail de sources plus large. Si le fichier est inconnu du service de réputation, le fichier est mis à la disposition de l'utilisateur, mais le résultat de l'analyse de fichier est mis à jour dans le cache local et est utilisé pour évaluer les instances futures du fichier dans .
- Si les informations de verdict de réputation de fichier ne sont pas disponibles parce que la connexion avec le serveur a expiré, le fichier est considéré comme non analysable et les actions configurées sont appliquées.

Fichiers à faible risque

Lorsqu'un fichier est initialement évalué comme inconnu et n'a aucun contenu dynamique, l'appliance l'envoie au moteur de préclassification, où il est désigné comme à faible risque. Ce fichier n'est pas téléchargé pour analyse. En cas d'accès au même fichier avant l'expiration du cache, il est à nouveau évalué comme à faible risque et n'est pas téléchargé pour analyse. Après l'expiration du délai du cache, en cas d'accès au même fichier, il est évalué comme inconnu et à faible risque dans l'ordre. Ce processus est répété pour les fichiers à faible risque. Puisque ces fichiers à faible risque ne sont pas chargés, ils ne feront pas partie des rapports d'analyse de fichiers.

Figure 9: Cisco Secure Endpoint Flux de travail pour les déploiements d'analyse de fichiers dans le nuage



Si le fichier est envoyé pour analyse :

- Si le fichier est envoyé dans le nuage pour analyse : les fichiers sont envoyés sur HTTPS.
- L'analyse prend normalement quelques minutes, mais peut être plus longues.
- Un fichier signalé comme malveillant après l'analyse du fichier peut ne pas être identifié comme malveillant par le service de réputation. La réputation d'un fichier est déterminée par divers facteurs au fil du temps, pas nécessairement par un seul verdict d'analyse de fichier.
- Les résultats des fichiers analysés à l'aide d'une appliance Cisco Secure Endpoint Malware Analytics sur site sont mis en cache localement.

Pour en savoir plus sur les mises à jour des verdicts, consultez Mises à jour des verdicts de menaces des fichiers , on page 324.

Fichiers pris en charge pour les services de réputation et d'analyse des fichiers

Le service de réputation évalue la plupart des types de fichiers. L'identification du type de fichier est déterminée par le contenu du fichier et ne dépend pas de l'extension du nom du fichier.

Certains fichiers de réputation inconnue peuvent être analysés pour connaître les caractéristiques des menaces. Lorsque vous configurez la fonction d'analyse des fichiers, vous choisissez les types de fichiers à analyser. De nouveaux types peuvent être ajoutés dynamiquement; vous recevrez une alerte lorsque la liste des types de fichiers téléchargeables sera modifiée et pourrez sélectionner les types de fichiers ajoutés à charger.

Les détails sur les fichiers pris en charge par les services de réputation et d'analyse ne sont disponibles que pour les clients enregistrés de Cisco. Pour en savoir plus sur les fichiers évalués et analysés, consultez *Critères des fichiers pour les services Advanced Malware Protection des produits Cisco Content Security*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html. Les critères d'évaluation de la réputation d'un fichier et d'envoi des fichiers pour analyse peuvent changer à tout moment.

Pour accéder à ce document, vous devez avoir un compte client Cisco avec un contrat d'assistance. Pour vous inscrire, consultez la page https://tools.cisco.com/RPF/register/register.do.

Votre paramètre pour **DVS Engine Object Scanning Limits** (Limites d'analyse des objets du moteur DVS) dans la page **Security Services > Anti-Malware and Reputation** (Services de sécurité> Antiprogrammes malveillants et réputation) détermine également la taille de fichier maximale pour la réputation et l'analyse des fichiers.

Vous devez configurer des politiques pour bloquer télécharger de fichiers qui ne sont pas adressés par Cisco Secure Endpoint.

Note Un fichier (se trouvant dans un courriel entrant ou sortant) qui a déjà été téléchargé pour analyse, quelle que soit la source, ne sera pas téléchargé à nouveau. Pour afficher les résultats de l'analyse pour un tel fichier, recherchez le SHA-256 dans la page de rapports d'analyse des fichiers.

Thèmes connexes

- Activation et configuration des services de réputation et d'analyse des fichiers , on page 332
- Veiller à recevoir des alertes sur les problèmes Cisco Secure Endpoint , on page 339
- Traitement d'archives ou de fichiers compressés, on page 326

Traitement d'archives ou de fichiers compressés

Si le fichier est compressé ou archivé,

- la réputation du fichier compressé ou d'archive est évaluée.
- Pour certains types de fichiers sélectifs, le fichier compressé ou d'archive est décompressé et la réputation de tous les fichiers extraits est évaluée.

Pour en savoir plus sur les fichiers archivés et compressés qui sont examinés, y compris les formats de fichier, consultez les informations liées à partir de Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 326.

Dans ce scénario,

- Si l'un des fichiers extraits est malveillant, le service File Reputation renvoie le verdict Malicious pour le fichier compressé ou l'archive.
- Si le fichier compressé ou d'archive est malveillant et que tous les fichiers extraits sont sains, le service de réputation des fichiers renvoie un verdict Malicious (Malveillant) pour le fichier compressé ou d'archive.
- Si le verdict de l'un des fichiers extraits est unknown, les fichiers extraits sont éventuellement (s'ils sont configurés et que le type de fichier est pris en charge pour l'analyse de fichier) envoyés pour analyse de fichier.
- Si l'extraction d'un fichier échoue lors de la décompression d'un fichier compressé ou d'une archive, le service File Reputation renvoie le verdict Non analysable pour le fichier compressé ou l'archive. N'oubliez pas que, dans ce scénario, si l'un des fichiers extraits est malveillant, le service de réputation des fichiers renvoie un verdict de malveillance pour le fichier compressé ou l'archive (le verdict de malveillance prévaut sur le verdict Non analysable).
- Un fichier compressé ou d'archive est traité comme non analysable dans les scénarios suivants :
  - Le taux de compactage des données est supérieur à 20.
  - Le fichier d'archive contient plus de cinq niveaux d'imbrication.
  - Le fichier d'archive contient plus de 200 fichiers enfants.
  - La taille du fichier d'archive dépasse 50 Mo.
  - Le fichier d'archive est protégé par un mot de passe ou illisible.

Note La réputation des fichiers extraits avec des types MIME sécurisés, par exemple, texte/brut, n'est pas évaluée.

Confidentialité des informations envoyées dans le nuage

- Seul le SHA qui identifie de manière unique un fichier est envoyé au service de réputation dans le nuage. Le fichier proprement dit n'est pas envoyé.
- Si vous utilisez le service d'analyse de fichier dans le nuage et qu'un fichier est admissible pour l'analyse, le fichier proprement dit est envoyé dans le nuage.
- Les informations sur chaque fichier envoyé dans le nuage pour analyse et ayant un verdict « malveillant » sont ajoutées à la base de données de réputation. Ces renseignements sont utilisés avec d'autres données pour déterminer un score de réputation.

  Les renseignements sur les fichiers analysés par une appliance Cisco Secure Endpoint Malware Analytics sur site ne sont pas partagés avec le service de réputation.

Configuration des fonctionnalités d'analyse et de réputation de fichiers

Exigences de communication avec les services de réputation et d'analyse de fichiers

- Toutes les appliances Secure Web Appliance qui utilisent ces services doivent pouvoir s'y connecter directement par Internet (à l'exception des services d'analyse des fichiers configurés pour utiliser une appliance Cisco Secure Endpoint Malware Analytics sur site).
- Par défaut, la communication avec les services de réputation et d'analyse des fichiers est acheminée par le port de gestion (M1) sur l'appliance. Si votre appliance n'achemine pas de données par le port de gestion, consultez Routage du trafic vers les serveurs d'analyse des fichiers et de réputation de fichier par une interface de données , on page 329.
- Par défaut, la communication avec les services de réputation de fichiers et d'analyse en nuage est acheminée par l'interface associée à la passerelle par défaut. Pour acheminer ce trafic par l'intermédiaire d'une interface différente, créez une voie de routage statique pour chaque adresse dans la section avancée de la page Security Services > File Reputation and Analysis (Services de sécurité > Réputation et analyse des fichiers).
- Les ports de pare-feu suivants doivent être ouverts :

Ports de pare-feu	Description	Protocole	Entrée/Sortie	Hostname (Nom d'hôte)	Interface de l'appliance
32137 (par défaut) ou 443	L'accès aux services Cisco Cloud pour obtenir la réputation de fichier.	TCP	Sortant	Comme configuré dans Security Services > Anti-Malware and Reputation, Advanced section: Advanced Settings for File Reputation (Services de sécurité > Antiprogrammes malveillants et réputation, section Avancé : Paramètre avancé pour la réputation des fichiers), paramètre Cloud Server Pool (Regroupement de serveurs sur le nuage).	Management (Gestion), sauf si une voie de routage statique est configurée pour acheminer ce trafic par un port de données.
443	Accès aux services en nuage pour l'analyse de fichiers.	TCP	Sortant	Comme configuré dans Security Services > Anti-Malware and Reputation, Advanced section: Advanced Settings for File Analysis (Services de sécurité > Antiprogrammes malveillants et réputation, section Avancé : Paramètres avancés pour l'analyse des fichiers).	

- Lorsque vous configurez la fonction de réputation de fichiers, choisissez si vous souhaitez utiliser SSL sur le port 443.

Thèmes connexes

- Activation et configuration des services de réputation et d'analyse des fichiers

Routage du trafic vers les serveurs d'analyse des fichiers et de réputation de fichier par une interface de données

Si l'appliance est configurée pour restreindre le port de gestion aux services de gestion de l'appliance uniquement [sur la page **Network > Interfaces** (Réseau > Interfaces)], configurez plutôt l'appliance pour acheminer le trafic d'analyse des fichiers et de réputation par le port de données.

Ajoutez des voies de routage pour le trafic de données sur la page Network > Routes (Réseau > Voies de routage). Pour connaître la configuration requise et les instructions générales, consultez Configuration des routages de trafic TCP/IP, on page 43.

Pour la connexion à	Réseaux de destination	Passerelle
Le service de réputation des fichiers	Dans Security Services > Anti-Malware and Reputation (Services de sécurité > Protection contre les programmes malveillants et réputation), section Advanced (Avancé) > section Advanced Settings for File Reputation (Paramètres avancés pour la réputation des fichiers), indiquez le nom (URL) du **serveur de réputation des fichiers** et le nom de **domaine dans le nuage** du regroupement de serveurs en nuage. Si vous choisissez Private Cloud (Cloud privé) pour le serveur de réputation des fichiers, saisissez le nom d'hôte ou l'adresse IP du serveur et indiquez une clé publique valide. Il doit s'agir de la même clé que celle utilisée par l'appliance du cloud privé. Nom d'hôte du regroupement de serveurs en nuage, tel que configuré dans les services de sécurité ; Protection contre les programmes malveillants et réputation, section Avancé : paramètres avancés pour la réputation des fichiers.	Adresse IP de la passerelle pour le port de données
Le service d'analyse de fichiers	• Dans Security Services > Anti-Malware and Reputation (Services de sécurité > Protection contre les programmes malveillants et réputation), section Advanced (Avancé) > section Advanced Settings for File Analysis (Paramètres avancés pour la réputation des fichiers), indiquez le nom (URL) du **serveur d'analyse des fichiers**. Si vous choisissez Private Cloud (Cloud privé) pour le serveur d'analyse des fichiers, saisissez l'URL du serveur et indiquez une autorité de certification valide. • L'ID du client d'analyse des fichiers est l'ID client de cette appliance sur le serveur d'analyse des fichiers (lecture seule). Le nom d'hôte du serveur d'analyse des fichiers, tel que configuré dans les services de sécurité; logiciel contre les programmes malveillants et réputation, section Avancé : Paramètres avancés pour l'analyse des fichiers.	Adresse IP de la passerelle pour le port de données

Thèmes connexes

• Configuration des routages de trafic TCP/IP, on page 43

Configuration d'un serveur de réputation de fichiers sur site

Si vous prévoyez d'utiliser une appliance Cisco Secure Endpoint Cisco Virtual Private Cloud en tant que serveur d'analyse de fichiers en nuage privé :

- Vous pouvez obtenir la documentation de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud, le guide d'installation et de configuration de FireAMP Private Cloud, à l'adresse http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html

  Utilisez cette documentation pour effectuer les tâches décrites dans cette rubrique.

  Vous pouvez accéder à de la documentation supplémentaire en cliquant sur le lien Help (Aide) sur l'appliance Cisco Secure Endpoint Virtual Private Cloud.
- Installez et configurez l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud en mode « proxy » ou « air-gap » (local).
- Vérifiez que la version logicielle de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud est 2.2, ce qui permet l'intégration avec l' Secure Web Appliance.
- Téléchargez le certificat et les clés Cisco Secure Endpoint Virtual Private Cloud sur cette appliance pour les charger dans cette Secure Web Appliance.

Remarque Après avoir configuré le serveur de réputation de fichier sur site, vous configurerez la connexion à partir de cette Secure Web Appliance. Voir l'étape 6 de Activation et configuration des services de réputation et d'analyse des fichiers , à la page 332

Configuration d'un serveur d'analyse de fichiers sur site

Si vous utilisez une appliance Cisco Secure Endpoint Malware Analytics en tant que serveur d'analyse de fichiers en nuage privé :

- Procurez-vous le Guide d'installation et de configuration de l'appliance Cisco Secure Endpoint Malware Analytics et le Guide d'administration de l'appliance Cisco Secure Endpoint Malware Analytics. La documentation de l'appliance Cisco Secure Endpoint Malware Analytics est disponible sur https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html.

  Utilisez cette documentation pour effectuer les tâches décrites dans cette rubrique.

  De la documentation supplémentaire est accessible à partir du lien Help (Aide) sur l'appliance Cisco Secure Endpoint Malware Analytics.

  Dans le Guide d'administration, recherchez des informations sur tous les points suivants : les intégrations avec d'autres appliances Cisco, CSA, l'API Cisco Sandbox Secure Web Appliance.
- Installez et configurez l'appliance Cisco Secure Endpoint Malware Analytics.
- Au besoin, mettez à jour le logiciel de vos appliances Cisco Secure Endpoint Malware Analytics vers la version 1.2.1, qui prend en charge l'intégration avec Secure Web Appliance.

  Consultez la documentation de Cisco Secure Endpoint Malware Analytics pour obtenir des instructions sur la façon de déterminer le numéro de version et d'effectuer la mise à jour.

- Vérifiez que vos appliances peuvent communiquer entre elles sur votre réseau. Les Secure Web Appliance doivent pouvoir se connecter à l'interface SAINE de l'appliance Cisco Secure Endpoint Malware Analytics.
- Si vous souhaitez déployer un certificat autosigné : générez un certificat SSL autosigné à partir de l'appliance Cisco Secure Endpoint Malware Analytics à utiliser sur votre Secure Web Appliance. Consultez les instructions pour le téléchargement des clés et des certificats SSL dans le guide de l'administrateur de votre appliance Cisco Secure Endpoint Malware Analytics. Assurez-vous de générer un certificat indiquant CN comme nom d'hôte de votre appliance Cisco Secure Endpoint Malware Analytics. Le certificat par défaut de l'appliance Cisco Secure Endpoint Malware Analytics ne fonctionne PAS.
- L'enregistrement de votre Secure Web Appliance sur votre appliance Malware Analytics se produit automatiquement lorsque vous envoyez la configuration pour l'analyse des fichiers, comme décrit dans Activation et configuration des services de réputation et d'analyse des fichiers . Cependant, vous devez activer l'enregistrement comme décrit dans la même procédure.

Note Après avoir configuré le serveur d'analyse de fichiers sur site, vous configurerez la connexion à partir de ce Secure Web Appliance; consultez l'étape 7 de la section Activation et configuration des services de réputation et d'analyse des fichiers .

Activation et configuration des services de réputation et d'analyse des fichiers

Before you begin

- Obtenez des clés de fonctionnalité pour le service de réputation des fichiers et le service d'analyse des fichiers, et les transférer vers cet appliances. Consultez Utilisation des clés de fonctionnalité, on page 559 pour en savoir plus sur l'ajout de clés de fonctionnalité à l'appliance.
- Rencontrez les Exigences de communication avec les services de réputation et d'analyse de fichiers , on page 328.
- Assurez-vous qu'une interface réseau de données est activée sur l'appliance si vous souhaitez utiliser une interface réseau de données pour les services de réputation et d'analyse des fichiers. Voir la section Activation ou modification des interfaces réseau, on page 27.
- Vérifiez la connectivité aux serveurs de mise à jour configurés (Mises à jour) dans Configuration des paramètres de mise à niveau et de mise à jour de services, on page 619.
- Si vous souhaitez utiliser une appliance Cisco Cisco Secure Endpoint Virtual Private Cloud comme serveur de réputation des fichiers dans le nuage privé, consultez Configuration d'un serveur de réputation de fichiers sur site, on page 331.
- Si vous utilisez une appliance Cisco Secure Endpoint Malware Analytics en tant que serveur d'analyse de fichiers dans un nuage privé, consultez Configuration d'un serveur d'analyse de fichiers sur site , on page 331.

Étape 1 Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants > Réputation et analyse des fichiers).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cliquez sur **Enable File Reputation Filtering** (Activer le filtrage de la réputation des fichiers) et éventuellement sur **Enable File Analysis** (Activer l'analyse des fichiers).

- Si l'option **Enable File Reputation Filtering** (Activer le filtrage de réputation des fichiers) est cochée, vous devez configurer la section **File Reputation Server** (Serveur de réputation des fichiers) (à l'**étape 6**), en choisissant l'URL d'un serveur de réputation externe sur un nuage public ou en fournissant les informations de connexion au serveur de réputation sur un nuage privé.
- De même, si l'option **Enable File Analysis** (Activer l'analyse des fichiers) est cochée, vous devez configurer la section **File Analysis Server URL** (URL du serveur d'analyse des fichiers) (à l'**étape 7**), en indiquant l'URL d'un serveur sur un nuage externe ou les informations de connexion au nuage d'analyse privé.

Note De nouveaux types de fichiers peuvent être ajoutés après une mise à niveau et ne sont pas activés par défaut. Si vous avez activé l'analyse des fichiers et que vous souhaitez inclure les nouveaux types de fichiers dans l'analyse, vous devez les activer.

Étape 4 Acceptez le contrat de licence, s'il s'affiche.

Étape 5 Dans la section **File Analysis** (Analyse des fichiers), sélectionnez les types de fichiers requis dans les groupes de fichiers appropriés (par exemple, « documents Microsoft ») afin de les envoyer pour analyse.

Pour en savoir plus sur les types de fichiers pris en charge, consultez le document décrit dans Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 326

Étape 6 Développez le volet **Advanced Settings for File Reputation** (Paramètres avancés pour la réputation des fichiers) et ajustez les options suivantes, si nécessaire :

Option	Description
Cloud Domain (Domaine en nuage)	Nom du domaine à utiliser pour les requêtes de réputation de fichiers.
File Reputation Server (Serveur de réputation des fichiers)	Choisissez : le nom d'hôte du serveur de réputation en nuage public ou le nuage de réputation privé. Si vous choisissez un nuage de réputation privé, indiquez les informations suivantes : • **Server** (Serveur) : nom d'hôte ou adresse IP de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud. • **Public Key** (Clé publique) : indiquez une clé publique valide pour les communications chiffrées entre cette appliance et votre appliance en nuage privé. Il doit s'agir de la même clé que celle utilisée par le serveur en nuage privé : localisez le fichier de clé sur cette appliance, puis cliquez sur **Upload File** (Charger le fichier). **Note** Vous devez avoir déjà téléchargé le fichier de clé du serveur vers cette appliance.
Routing Table (Tableau de routage)	Table de routage (associée à un type d'interface réseau d'appliance, de gestion ou de données) à utiliser pour les services Cisco Secure Endpoint. Si l'appliance est à la fois une interface de gestion et une ou plusieurs interfaces de données activées, vous pouvez sélectionner Management (Gestion) ou Data (Données).

Option	Description
SSL Communication for File Reputation (Communication SSL pour la réputation des fichiers)	Cochez la case **Use SSL (Port 443)** [Utiliser SSL (Port 443)] pour communiquant sur le port 443 au lieu du port par défaut 32137. Consultez le guide de l'utilisateur de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud pour obtenir des renseignements sur l'activation de l'accès SSH au serveur. **Note** La communication SSL sur le port 32137 peut vous obliger à ouvrir ce port dans votre pare-feu. Cette option vous permet également de configurer un proxy en amont pour la communication avec le service de réputation des fichiers. Si cette option est cochée, renseignez comme approprié les champs **Server** (Serveur), **Username** (Nom d'utilisateur) et **Passphrase** (Phrase secrète). Si l'option **Use SSL (Port 443)** [Utiliser SSL (Port 443)] est sélectionnée, vous pouvez aussi cocher la case **Relax Certificate Validation** (Assouplir la validation des certificats) pour ignorer la validation de certificat standard si le certificat du serveur proxy de tunnel n'est pas signé par une autorité racine approuvée. Par exemple, sélectionnez cette option si vous utilisez un certificat autosigné sur un serveur proxy de tunnel interne approuvé. **Note** Si vous avez coché l'option **Use SSL (Port 443)** [Utiliser SSL (Port 443)] dans la section SSL Communication for File Reputation (Communication SSL pour la réputation des fichiers) des paramètres avancés pour la réputation des fichiers, vous devez ajouter le certificat de l'autorité de certification du serveur de réputation sur site Cisco Secure Endpoint au magasin de certificats de cette appliance, en utilisant Network > Certificates (Custom Certificate Authorities) [Réseau > Certificats (Autorités de certification personnalisées)] dans l'interface Web. Obtenez ce certificat auprès du serveur [Configuration > SSL > Cloud server > download (Configuration > SSL > Serveur en nuage > télécharger)].
Heartbeat Interval (Intervalle entre les pulsations)	Fréquence, en minutes, à laquelle envoyer un message Ping pour les événements rétrospectifs.
Query Timeout (Délai d'expiration de la requête)	Nombre de secondes écoulées avant l'expiration de la requête de réputation.
File Reputation Client ID (ID du client de réputation des fichiers)	ID de client pour cette appliance sur le serveur de réputation des fichiers (lecture seule).

Note Ne modifiez aucun autre paramètre dans cette section sans l'aide de l'assistance Cisco.

Étape 7 Si vous comptez utiliser le service en nuage pour l'analyse des fichiers, développez le volet Advanced Settings for File Analysis (Paramètres avancés pour l'analyse des fichiers) et réglez les options suivantes au besoin :

Option	Description
File Analysis Server URL (URL du serveur d'analyse des fichiers)	Choisissez : le nom (URL) d'un serveur en nuage externe ou le **Private analysis cloud** (Nuage d'analyse privé). Si vous indiquez un serveur en nuage externe, choisissez le serveur qui est physiquement le plus proche de votre appliance. Les nouveaux serveurs disponibles seront ajoutés à cette liste régulièrement à l'aide des processus de mise à jour standard. Choisissez Private analysis cloud (Nuage d'analyse privé) pour utiliser une appliance Cisco Secure Endpoint Malware Analytics sur site pour l'analyse des fichiers et saisissez les informations suivantes : • **TG Servers** (Serveurs TG) : saisissez l'adresse IPv4 ou le nom d'hôte des appliances Cisco Secure Endpoint Malware Analytics, autonomes ou en grappe. Vous pouvez ajouter au maximum sept appliances Cisco Secure Endpoint Malware Analytics. **Note** Le numéro de série indique l'ordre dans lequel vous ajoutez les appliances Cisco Secure Endpoint Malware Analytics autonomes ou en grappe. Il ne désigne pas la priorité des appliances. **Note** Vous ne pouvez pas ajouter de serveurs autonomes et de serveurs en grappe dans une seule instance. Ils doivent être autonomes ou en grappe. Vous ne pouvez ajouter qu'un seul serveur autonome par instance. En mode grappe, vous pouvez ajouter jusqu'à sept serveurs et tous les serveurs doivent appartenir à la même grappe. Vous ne pouvez pas ajouter plusieurs grappes. • **Certificate Authority** (Autorité de certification) : sélectionnez **Use Cisco Default Certificate Authority** (Utiliser l'autorité de certification par défaut de Cisco) ou **Use Uploaded Certificate Authority** (Utiliser l'autorité de certification chargée). Si vous choisissez **Use Uploaded Certificate Authority** (Utiliser l'autorité de certification chargée) et cliquez sur **Browse** (Parcourir) pour charger un fichier de certificat valide pour les communications chiffrées entre cette appliance et votre appliance de nuage privé. Il doit s'agir du même certificat utilisé par le serveur en nuage privé. **Note** Si vous avez configuré le portail Cisco Secure Endpoint Malware Analytics sur votre appliance pour l'analyse des fichiers, vous pouvez accéder au portail Cisco Secure Endpoint Malware Analytics (par exemple, https://panacea.threatgrid.eu) pour afficher et suivre les fichiers soumis pour l'analyse des fichiers. Pour en savoir plus sur l'accès au portail de Cisco Secure Endpoint Malware Analytics, communiquez avec le centre d'assistance technique de Cisco.

Option	Description
Proxy Settings (Paramètres de proxy)	Cochez la case **Use File Reputation Proxy** (Utiliser le proxy de réputation des fichiers) pour utiliser le même tunnel de proxy de réputation des fichiers que vous avez déjà configuré comme proxy en amont pour l'analyse des fichiers. Si vous souhaitez configurer un autre proxy en amont, décochez la case **Use File Reputation Proxy** (Utiliser le proxy de réputation des fichiers) et saisissez les informations appropriées dans les champs **Server** (Serveur), **Port**, **Username** (Nom d'utilisateur) et **Passphrase** (Phrase secrète).
File Analysis Client ID (ID du client d'analyse de fichier)	ID de client pour cette appliance sur le serveur d'analyse des fichiers (lecture seule).

Étape 8 (Facultatif) Développez le volet Cache Settings (Paramètres de cache) si vous souhaitez configurer la période d'expiration du cache pour les valeurs de disposition de réputation des fichiers.

Étape 9 Développez le volet Threshold Settings (Paramètres de seuil) si vous souhaitez définir la limite supérieure du score d'analyse de fichier acceptable. Le score au-dessus de ce seuil indique que le fichier est infecté. Choisissez l'une des options suivantes :

- Use value from Cloud Service (95) [Utiliser la valeur du service en nuage (95)]
- Enter Custom Value (Saisissez une valeur personnalisée) : par défaut, 95

Note L'option **Threshold Settings** (Paramètres de seuil) est désormais classée comme **File Analysis Threshold** (Seuil d'analyse de fichier) plutôt que comme **Reputation Threshold** (Seuil de réputation).

Étape 10 Envoyez et validez vos modifications.

Étape 11 Si vous utilisez une appliance Cisco Secure Endpoint Malware Analytics sur site, activez le compte pour cette appliance sur l'appliance Cisco Secure Endpoint Malware Analytics.

Des instructions complètes sur l'activation du compte « utilisateur » sont disponibles dans la documentation de Cisco Secure Endpoint Malware Analytics.

a) Notez l'ID du client d'analyse de fichiers qui s'affiche au bas de la section de la page. Cela identifie « l'utilisateur » que vous activerez.
b) Connectez-vous à l'appliance Cisco Secure Endpoint Malware Analytics.
c) Sélectionnez **Welcome... > Manage Users** (Bienvenue... > Gérer les utilisateurs) et accédez aux détails de l'utilisateur.
d) Localisez le compte « utilisateur » en fonction de l'ID de client d'analyse de fichier de vos Secure Web Appliance.
e) Activez ce compte « utilisateur » pour votre appliance.

Important! Modifications nécessaires dans le paramètre d'analyse de fichiers

Si vous prévoyez d'utiliser un nouveau service d'analyse de fichiers public dans le nuage, assurez-vous de lire les instructions suivantes pour maintenir l'isolement du centre de données :

- Les informations sur le regroupement d'appliances existants ne sont pas conservées dans le nouveau serveur d'analyse de fichiers. Vous devez regrouper vos appliances sur le nouveau serveur d'analyse de fichiers.

- Les messages mis en quarantaine dans la quarantaine d'analyse des fichiers sont conservés jusqu'à la période de conservation. Après la période de conservation en quarantaine, les messages sont libérés de la quarantaine d'analyse de fichiers et analysés de nouveau par le moteur Cisco Secure Endpoint . Le fichier est ensuite téléchargé sur le nouveau serveur d'analyse de fichiers pour analyse, mais le message n'est pas de nouveau envoyé en quarantaine d'analyse de fichiers.

Pour plus de détails, consultez la documentation de Cisco Cisco Secure Endpoint Malware Analytics de https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html.

(Services d'analyse des fichiers dans le nuage public uniquement) Configuration des groupes d'appliances

Pour permettre à toutes les appliances de sécurité de contenu de votre organisation d'afficher les détails des résultats de l'analyse des fichiers dans le nuage pour les fichiers envoyés pour analyse à partir de n'importe quelle appliance de votre organisation, vous devez joindre toutes les appliances au même groupe d'appliances.

Note Vous pouvez configurer des groupes d'appliances au niveau de l'ordinateur. Les groupes d'appliances ne peuvent pas être configurés au niveau de la grappe.

Étape 1 Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation > Analyse de réputation et des fichiers).

Étape 2 [S'applique si la licence Smart est désactivée sur votre passerelle de messagerie] Saisissez manuellement l'ID de groupe dans le champ **Appliance ID/Name** (ID/Nom de l'appliance) et cliquez sur **Group Now** (Regrouper maintenant).

Ou

[Applicable si la licence Smart est activée sur votre passerelle de messagerie] Le système enregistre automatiquement l'ID de compte Smart en tant qu'ID de groupe et l'affiche dans le champ **Appliance Group ID/Name** (ID/Nom du groupe d'appliances).

Remarques :

- Une appliance ne peut appartenir qu'à un seul groupe.
- Vous pouvez ajouter un ordinateur à un groupe à tout moment.
- Vous pouvez configurer des groupes d'appliances au niveau de l'ordinateur et de la grappe.
- S'il s'agit de la première appliance ajoutée au groupe, indiquez un identifiant utile pour le groupe. Cet ID est sensible à la casse et ne peut pas contenir d'espaces.
- L'ID de groupe d'appliances que vous fournissez doit être identique sur toutes les appliances qui partageront des données sur les fichiers téléchargés à des fins d'analyse. Cependant, l'ID n'est pas validé sur les appliances suivantes du groupe.
- Si vous mettez à jour l'ID de groupe d'appliances, la modification prend effet immédiatement et ne nécessite pas de validation.
- Vous devez configurer toutes les appliances d'un groupe pour utiliser le même serveur d'analyse de fichiers dans le nuage.
- Si les licences Smart sont activées, les appliances sont regroupées en utilisant l'ID de compte Smart.

Étape 3 Dans la section Appliance Grouping for Cloud Reporting Cloud (Regroupement d'appliances pour la création de rapports en nuage), saisissez l'ID du groupe de rapports d'analyse de fichiers dans le nuage.

- S'il s'agit de la première appliance ajoutée au groupe, indiquez un identifiant utile pour le groupe.
- Cet ID est sensible à la casse et ne peut pas contenir d'espaces.
- L'ID que vous indiquez doit être identique sur toutes les appliances qui partageront des données sur les fichiers téléchargés pour analyse. Cependant, l'ID n'est pas validé sur le groupe d'appliances suivant.
- Si vous saisissez l'ID de groupe incorrectement ou si vous devez le changer pour toute autre raison, vous devez ouvrir un dossier auprès du service d'assistance technique de Cisco.
- Cette modification prend effet immédiatement; elle ne nécessite pas de validation.
- Toutes les appliances du groupe doivent être configurées pour utiliser le même serveur d'analyse de fichiers dans le nuage.
- Une appliance ne peut appartenir qu'à un seul groupe.
- Vous pouvez ajouter un ordinateur à un groupe à tout moment, mais vous ne pouvez le faire qu'une seule fois.

Étape 4 Cliquez sur **Add Appliance to Group** (Ajouter l'appliance au groupe).

Quelles appliances se trouvent dans le groupe d'analyse?

Étape 1 Sélectionnez **Security Services> Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation).

Étape 2 Dans la section Appliance Grouping for File Analysis Cloud Reporting (Groupe d'appliances pour la création de rapports en nuage sur l'analyse des fichiers), cliquez sur **View Appliances in Group** (Afficher les appliances dans le groupe).

Étape 3 Pour afficher l'**ID du client d'analyse de fichiers** d'une appliance particulière, consultez l'emplacement suivant :

Appareil	Emplacement de l'ID du client d'analyse des fichiers
Appliance de sécurité de la messagerie	Section Advanced Settings for File Analysis (Paramètres avancés pour l'analyse des fichiers) sur la page **Security Services > File Reputation and Analysis** (Services de sécurité > Réputation et analyse des fichiers).
Secure Web Appliance	Advanced Settings for File Analysis (Paramètres avancés pour l'analyse des fichiers) sur la page **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation)
Appliance de gestion de la sécurité	Au bas de la page **Management Appliance > Centralized Services > Security Appliances** (Appliance de gestion > Services centralisés > Appliances de sécurité).

Configuration de l'action du service de réputation et d'analyse des fichiers par politique d'accès

Étape 1 Sélectionnez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans la colonne **Anti-Malware and Reputation** (Protection contre les programmes malveillants et réputation) correspondant à une politique dans le tableau.

Étape 3 Dans la section **Cisco Secure Endpoint Settings** (Paramètres Cisco Secure Endpoint), sélectionnez **Enable File Reputation Filtering and File Analysis** (Activer le filtrage de réputation de fichiers et l'analyse de fichiers).

Si l'analyse de fichiers n'est pas activée globalement, seul le filtrage de réputation de fichier est proposé.

Étape 4 Sélectionnez une action pour **Known Malicious and High-Risk Files** (Fichiers malveillants ou à haut risque connus) : **Monitor** (Superviser) ou **Block** (Bloquer).

La valeur par défaut est Monitor (Superviser).

Étape 5 Envoyez et validez vos modifications.

Veiller à recevoir des alertes sur les problèmes Cisco Secure Endpoint

Vérifiez que l'appliance est configurée pour vous envoyer des alertes relatives à Cisco Secure Endpoint.

Vous recevrez des alertes dans les cas suivants :

Description de l'alerte	Type	Gravité
Vous configurez une connexion à une appliance Cisco Secure Endpoint Malware Analytics sur site (nuage privé) et vous devez activer le compte comme décrit dans la section Activation et configuration des services de réputation et d'analyse des fichiers .	Protection contre les programmes malveillants	Avertissement
Les clés de fonctionnalité expirent	(Comme pour toutes les fonctionnalités)	
Le service de réputation de fichiers ou d'analyse de fichiers est inaccessible.	Protection contre les programmes malveillants	Avertissement
La communication avec les services infonuagiques est établie.	Protection contre les programmes malveillants	Information
		Information
Un verdict de réputation de fichier change.	Protection contre les programmes malveillants	Information
Les types de fichiers pouvant être envoyés pour analyse ont été modifiés. Vous souhaiterez peut-être activer le chargement de nouveaux types de fichiers.	Protection contre les programmes malveillants	Information

Description de l'alerte	Type	Gravité
L'analyse de certains types de fichiers est temporairement indisponible.	Protection contre les programmes malveillants	Avertissement
L'analyse de tous les types de fichiers pris en charge est restaurée après une panne temporaire.	Protection contre les programmes malveillants	Information
Clé de service d'analyse de fichiers non valide. Vous devez contacter le service d'assistance technique de Cisco avec les détails d'ID de l'analyse des fichier pour corriger cette erreur.	Cisco Secure Endpoint	Erreur

Thèmes connexes

- Plusieurs alertes concernant l'échec de la connexion aux serveurs d'analyse ou de réputation des fichiers , on page 345
- Mesures à prendre lors de changements de verdicts des menaces de fichiers , on page 344

Configuration de rapports centralisés pour les fonctionnalités Cisco Secure Endpoint

Si vous souhaitez centraliser les rapports sur une appliance de gestion de la sécurité, consultez les exigences de configuration importantes décrites aux sections Cisco Secure Endpoint de la rubrique relative aux rapports par dans l'aide en ligne ou le guide de l'utilisateur de votre appliance de gestion.

Création de rapports et suivi de la réputation et de l'analyse des fichiers

- Identification des fichiers par algorithme de hachage SHA-256 , on page 340
- Pages de rapport de réputation et d'analyse des fichiers, on page 341
- Affichage des données de filtrage de réputation des fichiers dans d'autres rapports , on page 342
- À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint , on page 343

Identification des fichiers par algorithme de hachage SHA-256

Comme les noms de fichiers peuvent être facilement modifiés, l'appliance génère un identifiant pour chaque fichier à l'aide d'un algorithme de hachage sécurisé (SHA-256). Si une appliance traite le même fichier avec des noms différents, toutes les instances sont reconnues comme ayant le même SHA-256. Si plusieurs appliances traitent le même fichier, toutes les instances du fichier ont le même identifiant SHA-256.

Dans la plupart des rapports, les fichiers sont répertoriés en fonction de leur valeur SHA-256 (dans un format abrégé). Pour identifier les noms de fichiers associés à une instance de programme malveillant dans votre

entreprise, sélectionnez Reporting (Rapports) > Cisco Secure Endpoint et cliquez sur un lien SHA-256 dans le tableau. La page de détails affiche les noms de fichiers associés.

Pages de rapport de réputation et d'analyse des fichiers

Rapport	Description
Cisco Secure Endpoint	Affiche les menaces basées sur les fichiers qui ont été identifiées par le service de réputation des fichiers. Pour les fichiers dont les verdicts ont été modifiés, consultez le rapport sur les mises à jour des verdicts Cisco Secure Endpoint . Ces verdicts ne sont pas reflétés dans le rapport Cisco Secure Endpoint. Si un fichier extrait d'un fichier compressé ou archivé est malveillant, seule la valeur SHA du fichier compressé ou archivé est incluse dans le rapport Cisco Secure Endpoint. La section **Incoming Malware Files by Category** (Fichiers de programmes malveillants entrants par catégorie) indique le pourcentage d'informations SHA du fichier de la liste de blocage reçue de la console Cisco Secure Endpoint qui sont classées comme **Custom Detection** (Détection personnalisée). Le nom de menace du fichier SHA sur la liste de blocage reçue de la console Cisco Secure Endpoint est affiché comme **Simple Custom Detection** (Détection personnalisée simple) dans la section Incoming Malware Threat Files (Fichiers de programmes malveillants entrants) du rapport. Vous pouvez cliquer sur le lien dans la section More Details (Plus de détails) du rapport pour afficher les détails de la trajectoire du fichier au sujet des informations SHA du fichier dans la liste de blocage dans la console Cisco Secure Endpoint. Vous pouvez consulter les détails du verdict de **risque faible** dans la section Incoming Files Handed by Cisco Secure Endpoint (Fichiers entrants gérés par Cisco Secure Endpoint) du rapport.

Rapport	Description
Cisco Secure Endpoint File Analysis (Analyse des fichiers)	Affiche l'heure et le verdict (ou verdict provisoire) pour chaque fichier envoyé pour analyse. L'appliance vérifie les résultats de l'analyse toutes les 30 minutes. Pour afficher plus de 1000 résultats d'analyse des fichiers, exportez les données dans un fichier .csv. Accédez aux résultats détaillés de l'analyse, notamment les caractéristiques des menaces pour chaque fichier. Vous pouvez également rechercher des informations supplémentaires sur une valeur SHA ou cliquer sur le lien au bas de la page des détails de l'analyse des fichiers pour afficher des détails supplémentaires sur le serveur qui a analysé le fichier. **Remarque** Si des fichiers extraits d'un fichier compressé ou archivé sont envoyés pour analyse, seules les valeurs SHA de ces fichiers extraits sont incluses dans le rapport d'analyse des fichiers.
Cisco Secure Endpoint Reputation (Réputation)	Étant donné que Cisco Secure Endpoint est axé sur les menaces ciblées et de type « jour zéro », les verdicts sur les menaces peuvent changer à mesure que les données agrégées fournissent davantage d'informations. Le rapport de réputation Cisco Secure Endpoint répertorie les fichiers traités par cette appliance pour lesquels le verdict a changé depuis la réception du message. Pour plus d'informations sur cette situation, consultez Mises à jour des verdicts de menaces des fichiers , à la page 324. Pour afficher plus de 1000 mises à jour de verdicts, exportez les données dans un fichier .csv. Dans le cas de plusieurs modifications de verdicts pour un seul protocole SHA-256, ce rapport affiche uniquement le dernier verdict, et non l'historique des verdicts. Pour afficher tous les messages affectés par un protocole SHA-256 particulier pendant la plage de temps maximale disponible (quelle que soit la plage de temps sélectionnée pour le rapport), cliquez sur un lien SHA-256.

Affichage des données de filtrage de réputation des fichiers dans d'autres rapports

Les données relatives à la réputation et à l'analyse des fichiers sont disponibles dans d'autres rapports, le cas échéant. La colonne « Blocked by Cisco Secure Endpoint » (Bloqué par/Détecté par) peut être masquée par défaut dans les rapports applicables. Pour afficher d'autres colonnes, cliquez sur le lien Columns (Colonnes) sous le tableau.

Le rapport par emplacement utilisateur comprend un onglet Cisco Secure Endpoint.

À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint

Lorsque vous recherchez des informations sur les menaces liées aux fichiers dans le cadre du suivi Web, gardez à l'esprit les points suivants :

- Pour rechercher des fichiers malveillants trouvés par le service de réputation des fichiers, sélectionnez **Known Malicious and High-Risk Files** (Fichiers malveillants et à haut risque connus) pour l'option **Filter by Malware Category** (Filtrer par catégorie de programmes malveillants) dans la zone Malware Threat (Programmes malveillants) dans la section Advanced (Advanced) du suivi des messages Web.
- Le suivi des Web inclut uniquement des informations sur le traitement de réputation des fichiers et les verdicts de réputation de fichier initiaux renvoyés au moment du traitement d'un message de transaction. Par exemple, si un fichier a initialement été jugé sain, une mise à jour du verdict a révélé que le fichier est malveillant, seul le verdict sain s'affiche dans les résultats du suivi.

  Aucune information n'est fournie pour les pièces jointes propres ou non analysables.

  La mention « Block – AMP » dans les résultats de recherche signifie que la transaction a été bloquée en raison du verdict de réputation du fichier.

  Dans les détails du suivi, le « score de menace AMP » est le score le plus approprié fourni par le service de réputation en nuage quand un verdict clair concernant le fichier ne peut pas être déterminé. Dans cette situation, le score est compris entre 1 et 100. (Ignorez le score de menace AMP si un verdict Cisco Secure Endpoint est rendu ou si le score est de zéro .) L'appliance compare ce score au score du seuil (configuré sur la page Services de sécurité > Anti-Malware and Reputation) pour déterminer l'action à entreprendre. Par défaut, les fichiers renvoyant un score compris entre 60 et 100 sont considérés comme malveillants. Cisco ne recommande pas de modifier la note de seuil par défaut. Le score WBRS correspond à la réputation du site à partir duquel le fichier a été téléchargé; ce score n'est pas lié à la réputation du fichier.
- Les mises à jour de verdicts sont uniquement disponibles dans le rapport sur les mises à jour de verdicts Cisco Secure Endpoint . Les détails du message de d'origine dans le suivi des messages ne sont pas mis à jour avec les changements de verdict. Pour voir les transactions impliquant un fichier particulier, , cliquez sur un SHA-256 dans le rapport sur les mises à jour de verdicts.
- Les renseignements concernant l'analyse de fichier, notamment les résultats de l'analyse et l'envoi ou non d'un fichier pour analyse, sont uniquement accessibles dans le rapport d'analyse des fichiers.

  Des renseignements supplémentaires sur un fichier analysé peuvent être disponibles sur le serveur d'analyse de fichiers en nuage ou sur site. Pour afficher les informations d'analyse de fichier disponibles pour un fichier, sélectionnez le **Reporting > File Analysis** (Rapports > Analyse des fichiers) et saisissez SHA-256 pour rechercher le fichier ou cliquez sur le lien SHA-256 dans les détails du suivi Web. Si le service d'analyse des fichiers a analysé le fichier à partir de n'importe quelle source, vous pouvez voir les détails. Les résultats sont affichés uniquement pour les fichiers qui ont été analysés.

  Si l'appliance a traité une instance ultérieure d'un fichier qui a été envoyé pour analyse, ces instances apparaîtront dans les résultats de recherche du suivi des messages Web.

Mesures à prendre lors de changements de verdicts des menaces de fichiers

Étape 1 Affichez le rapport sur les mises à jour des verdicts de Cisco Secure Endpoint .

Étape 2 Cliquez sur le lien SHA-256 approprié pour afficher les données Web pour toutes les transactions impliquant des le fichier auquel les utilisateurs finaux ont été autorisés à accéder.

Étape 3 À l'aide des données de suivi, identifiez les utilisateurs qui pourraient être en danger, ainsi que des informations telles que les noms de fichiers impliqués dans l'incident et le site Web à partir duquel le fichier a été téléchargé.

Étape 4 Consultez le rapport d'analyse de fichier pour voir si ce SHA-256 a été envoyé pour analyse, afin de comprendre plus en détail la menace qu'implique le fichier.

What to do next

Thèmes connexes

Mises à jour des verdicts de menaces des fichiers , on page 324

Résolution des problèmes liés à la réputation et à l'analyse des fichiers

Fichiers de journalisation

Dans les journaux :

- `AMP` et `amp` font référence au service ou au moteur de réputation de fichiers.
- `Retrospective` fait référence aux mises à jour de verdict.
- `VRT` et `sandboxing` font référence au service d'analyse des fichiers.

Les informations sur Cisco Secure Endpoint, y compris l'analyse des fichiers, sont enregistrées dans les journaux d'accès ou dans les journaux du moteurCisco Secure Endpoint . Pour en savoir plus, consultez la rubrique sur la supervision de l'activité du système par le biais des journaux.

Dans le message de journal « Response received for file reputation query » (Réponse reçue à la requête de réputation de fichier), les valeurs possibles pour « upload action » sont les suivantes :

- 1 : SEND. Dans ce cas, vous devez envoyer le fichier pour analyse de fichier.
- 2 : DON'T SEND. Dans ce cas, vous n'envoyez pas le fichier pour analyse de fichier.
- 3 : SEND ONLY METADATA. Dans ce cas, vous envoyez uniquement les métadonnées, et non le fichier entier, à l'analyse de fichier.
- 0 : NO ACTION. Dans ce cas, aucune autre action n'est requise.

Plusieurs alertes concernant l'échec de la connexion aux serveurs d'analyse ou de réputation des fichiers

Problème

Vous recevez plusieurs alertes concernant des échecs de connexion aux services d'analyse ou d'analyse de réputation des fichiers dans le nuage. (Une seule alerte peut indiquer qu'un problème transitoire.)

Solution

- Assurez-vous d'avoir satisfait aux exigences mentionnées dans Exigences de communication avec les services de réputation et d'analyse de fichiers , on page 328.
- Vérifiez les problèmes de réseau qui pourraient empêcher l'appliance de communiquer avec les services en nuage.
- Augmentez la valeur du délai d'expiration de la requête :

  Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation/Réputation et analyse des fichiers). La valeur du délai d'expiration de la requête se trouve dans la zone des paramètres avancés de la section Cisco Secure Endpoint **Services**.

Erreur de clé API (analyse des fichiers sur site)

Problème

Vous recevez une alerte de clé API lorsque vous tentez d'afficher les détails du rapport d'analyse de fichiers ou l' Secure Web Appliance ne peut pas se connecter au serveur Cisco Secure Endpoint Malware Analytics pour charger les fichiers à analyser.

Solution

Cette erreur peut se produire si vous modifiez le nom d'hôte du serveur Cisco Secure Endpoint Malware Analytics et que vous utilisez un certificat autosigné par le serveur Cisco Secure Endpoint Malware Analytics, ainsi que dans d'autres circonstances éventuellement. Pour résoudre le problème :

- Générez un nouveau certificat à partir de l'appliance Cisco Secure Endpoint Malware Analytics qui porte le nouveau nom d'hôte.
- Chargez le nouveau certificat sur l'appliance Secure Web Appliance.
- Réinitialisez la clé API sur l'appliance Cisco Secure Endpoint Malware Analytics. Pour obtenir des instructions, consultez l'aide en ligne sur l'appliance Cisco Secure Endpoint Malware Analytics.

Thèmes connexes

- Activation et configuration des services de réputation et d'analyse des fichiers

Les fichiers ne sont pas chargés comme prévu

Problème

Les fichiers ne sont pas évalués ou analysés comme prévu. Il n'y a aucune alerte ou erreur manifeste.

Solution

Prenez en compte les éléments suivants :

- Le fichier peut avoir été envoyé pour analyse par une autre appliance et donc déjà être présent sur le serveur d'analyse des fichiers ou dans le cache de l'appliance qui traite le fichier.
- Vérifiez la limite de taille de fichier maximale configurée pour les **limites d'analyse des objets du moteur DVS** sur la page **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation). Cette limite s'applique aux fonctionnalités Cisco Secure Endpoint.

Les détails de l'analyse des fichiers dans le nuage sont incomplets

Problème

Les résultats complets de l'analyse des fichiers dans le nuage public ne sont pas disponibles pour les fichiers chargés à partir d'autres Secure Web Appliance de mon organisation.

Solution

Assurez-vous de regrouper toutes les appliances qui partageront les données de résultats de l'analyse des fichiers. Consultez (Services d'analyse des fichiers dans le nuage public uniquement) Configuration des groupes d'appliances , on page 337. Cette configuration doit être effectuée sur chaque appliance du groupe.

Alertes sur les types de fichiers pouvant être envoyés à des fins d'analyse

Problème

Vous recevez des alertes d'informations sur la gravité sur les types de fichiers qui peuvent être envoyés pour analyse des fichiers.

Solution

Cette alerte est envoyée lorsque les types de fichiers pris en charge changent ou lorsque l'appliance vérifie quels types de fichiers sont pris en charge. Cela peut se produire dans les cas suivants :

- Vous ou un autre administrateur modifiez les types de fichiers sélectionnés pour analyse.
- Les types de fichiers pris en charge changent temporairement en fonction de la disponibilité dans le service en nuage. Dans ce cas, la prise en charge des types de fichiers sélectionnés sur l'appliance sera restaurée dès que possible. Les deux processus sont dynamiques et ne nécessitent aucune action de votre part.
- L'appliance redémarre, par exemple dans le cadre d'une mise à niveau d'AsyncOS.

CHAPITRE 15

Gestion de l'accès aux applications Web

Cette rubrique contient les sections suivantes :

Survol de la gestion de l'accès aux applications Web

Le moteur Application Visibility and Control (AVC) vous permet de créer des politiques pour contrôler l'activité des applications sur le réseau sans avoir à cerner parfaitement la technologie sous-jacente de chaque application. Vous pouvez configurer les paramètres de contrôle des applications dans les groupes de politiques d'accès. Vous pouvez bloquer ou autoriser les applications individuellement ou en fonction du type d'application. Vous pouvez également appliquer des contrôles à des types d'applications particuliers.

Les politiques d'accès vous permettent de :

- Contrôler les comportements des applications.
- Contrôler la quantité de bande passante utilisée pour des types d'applications particuliers
- Informer les utilisateurs finaux lorsqu'ils sont bloqués
- Affecter des contrôles aux applications de messagerie instantanée, de blogue et de réseaux sociaux
- Indiquer les paramètres de demande de plage

Pour contrôler les applications à l'aide du moteur AVC , effectuez les tâches suivantes :

Tâche	Lien vers la tâche
Activer le moteur AVC	Activation du moteur AVC , on page 348
Définir les contrôles dans un groupe de politiques d'accès	Configuration des paramètres de contrôle des applications dans un groupe de politiques d'accès, on page 352

Tâche	Lien vers la tâche
Limiter la bande passante utilisée par certains types d'applications pour contrôler la congestion	Contrôle de la bande passante, on page 353
Autoriser le trafic de messagerie instantanée, mais interdire le partage de fichiers à l'aide de la messagerie instantanée	Contrôle du trafic de la messagerie instantanée, on page 355

Activation du moteur AVC

Activez le moteur AVC lorsque vous activez les contrôles d'utilisation acceptable.

Note Vous pouvez consulter l'activité d'analyse du moteur AVC dans le rapport de visibilité des applications sur la page Reporting > Application Visibility (Création de rapports > Visibilité des applications).

Étape 1 Choisissez **Security Services > Acceptable Use Controls** (Services de sécurité > Contrôles d'utilisation acceptable).

Étape 2 Cliquez sur **Enable** (Activer) ou **Edit Global Settings** (Modifier les paramètres globaux), selon l'état actuel des contrôles d'utilisation acceptable.

Étape 3 Assurez-vous que la case Enable Cisco Web Usage Controls (Activer Cisco Web Usage Controls) est cochée.

Étape 4 Dans le volet Acceptable Use Controls Service (Service de contrôles d'utilisation acceptable), sélectionnez **Cisco Web Usage Controls**, puis sélectionnez **Enable Application Visibility and Control** (Activer Application Visibility and Control).

Étape 5 Sélectionnez l'**action par défaut pour le service inaccessible** : **Monitor** (Superviser) ou **Block** (Bloquer).

Étape 6 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Mises à jour du moteur AVC et actions par défaut , on page 348
- Expérience de l'utilisateur lorsque les demandes sont bloquées par le moteur AVC , on page 349

Mises à jour du moteur AVC et actions par défaut

AsyncOS interroge périodiquement les serveurs de mise à jour pour connaître de nouvelles mises à jour pour tous les composants des services de sécurité, y compris le moteur AVC. Les mises à jour du moteur AVC peuvent inclure la prise en charge de nouveaux types d'applications et d'applications, ainsi que la mise à jour de la prise en charge des applications existantes si le comportement des applications change. En mettant à jour le moteur AVC entre les mises à jour de version AsyncOS, Secure Web Appliance reste flexible sans nécessiter de mise à niveau du serveur.

AsyncOS pour le Web attribue les actions par défaut suivantes à la politique d'accès globale :

- Par défaut, les nouveaux types d'applications sont **Monitor** (Superviser).
- nouveaux comportements d'applications, comme le transfert de blocage de fichiers au sein d'une application particulière; la valeur par défaut est **Moniteur**.
- Les nouvelles applications pour un type d'application existant par défaut au type d'application par défaut.

Note Dans la politique d'accès globale, vous pouvez définir l'action par défaut pour chaque type d'application, de sorte que les nouvelles applications introduites dans une mise à jour de moteur AVC héritent automatiquement de l'action par défaut spécifiée. Consultez Configuration des paramètres de contrôle des applications dans un groupe de politiques d'accès, on page 352.

Expérience de l'utilisateur lorsque les demandes sont bloquées par le moteur AVC

Lorsque le moteur AVC bloque une transaction, le proxy Web envoie une page de blocage à l'utilisateur final. Cependant, tous les sites Web n'affichent pas la page de blocage à l'utilisateur final; de nombreux sites Web affichent du contenu dynamique en utilisant JavaScript au lieu d'une page Web statique et il est peu probable qu'ils affichent la page de blocage. Les utilisateurs ne peuvent toujours pas télécharger correctement des données malveillantes, mais ils ne sont pas toujours informés par le site Web.

Note Lorsque le proxy HTTPS est désactivé et Webroot est :

- Activé : le moteur AVC peut être lancé ou non et renvoyer le verdict. La transaction sera traitée selon le verdict de l'analyseur.
- Désactivé : le moteur AVC sera lancé et renverra le verdict. La transaction sera traitée conformément au verdict de Cisco AVC.

Paramètres de contrôle d'application des politiques

Le contrôle des applications nécessite la configuration des éléments suivants :

Option	Description
Types d'applications	Catégorie qui contient une ou plusieurs applications.
Applications	Applications particulières dans un Type d'application.
Comportements des applications	Actions ou comportements particuliers que les utilisateurs peuvent effectuer dans une application et que les administrateurs peuvent contrôler. Toutes les applications n'incluent pas des comportements que vous pouvez configurer.

Vous pouvez configurer les paramètres de contrôle des applications dans les groupes de politiques d'accès. Dans la page **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès), cliquez sur le lien **Applications** du groupe de politiques que vous souhaitez configurer. Lors de la configuration des applications, vous pouvez choisir les actions suivantes :

Option	Description
Block (Bloquer)	Cette action est une action finale. Les utilisateurs ne peuvent pas afficher une page Web et une page de notification de l'utilisateur final s'affiche à la place
Monitor (Surperviser)	Cette action est une action intermédiaire. Le proxy Web continue de comparer la transaction aux autres paramètres de contrôle pour déterminer l'action finale à appliquer
Restrict (Limiter)	Cette action indique qu'un comportement d'application est bloqué. Par exemple, lorsque vous bloquez les transferts de fichiers pour une application de messagerie instantanée particulière, l'action pour cette application est Restreindre.
Bandwidth Limit (Limite de bande passante)	Pour certaines applications, comme Media et Facebook, vous pouvez limiter la bande passante disponible pour le trafic Web. Vous pouvez limiter la bande passante pour l'application elle-même et pour ses utilisateurs.

Thèmes connexes

- Paramètres des demandes de plages, on page 350
- Règles et directives pour la configuration du contrôle des applications , on page 351

Paramètres des demandes de plages

Lorsque les demandes de plage HTTP sont désactivées et qu'un fichier volumineux est téléchargé sur plusieurs flux, le package consolidé est analysé. Cela annule les avantages en termes de performance des utilitaires et des applications de gestion des téléchargements utilisés pour télécharger les objets volumineux.

Par ailleurs, lorsque l'option Range Request Forwarding (Transfert des demandes de plage) est activée (voir Configuration des paramètres du proxy Web, on page 73), vous pouvez contrôler la façon dont les demandes de plage entrantes sont traitées pour chaque politique. Ce processus, appelé « service d'octets », permet d'optimiser la bande passante en cas de demandes de fichiers volumineux.

Cependant, l'activation du transfert des demandes de plage peut interférer avec l'efficacité du moteur Application Visibility and Control (AVC) selon les politiques et peut compromettre la sécurité. Veuillez faire preuve de prudence et activer le transfert des demandes de plage HTTP uniquement si les avantages l'emportent sur les conséquences pour la sécurité.

Note Les paramètres de demande de plage ne sont disponibles que lorsque le transfert des demandes de plage est activé et qu'au moins une application est réglée sur Block (Bloquer), Restrict (Restreindre) ou Throttle (Limiter).

Paramètres des demandes de plages pour la politique

Paramètres des demandes de plages	• **Do not forward range requests** (Ne pas transférer les demandes de plage) : le client envoie une demande pour une plage particulière. Mais le Secure Web Appliance supprime l'en-tête de plage de la demande avant de l'envoyer au serveur cible. Le Secure Web Appliance analyse ensuite le fichier entier et envoie la plage d'octets au client. **Note** La première fois que le client envoie la demande de plage, Secure Web Appliance, attendant les demandes de plage ultérieures du client, envoie le fichier entier. Pour toute demande successive du même client ou d'un autre client, Secure Web Appliance ne fournit qu'une partie du contenu au client. • **Forward range Requests** (Transférer les demandes de plage) : le client envoie une demande pour une plage particulière. Le Secure Web Appliance envoie la même demande au serveur cible et reçoit un contenu partiel qui est ensuite renvoyé au client. Le Secure Web Appliance analyse uniquement le contenu partiel pour lequel les résultats de l'analyse pourraient ne pas être exacts.
Liste des exceptions	Vous pouvez spécifier des destinations de trafic qui sont dispensées de la sélection de transfert actuelle. En d'autres termes, si l'option **Do not forward range requests** (Ne pas transférer les demandes) est sélectionnée, vous pouvez spécifier les destinations pour lesquelles les demandes sont transférées. De même, lorsque l'option **Forward range requests** (Transférer les demandes de plage) est sélectionnée, vous pouvez spécifier les destinations pour lesquelles les demandes ne sont pas transférées.

Règles et directives pour la configuration du contrôle des applications

Tenez compte des règles et des instructions suivantes lors de la configuration des paramètres de contrôle des applications :

- Les types d'applications pris en charge, les applications et les comportements des applications peuvent changer entre les mises à niveau d'AsyncOS pour le Web ou après les mises à jour du moteur AVC .
- Si vous activez la recherche sécurisée ou l'évaluation du contenu du site, le moteur AVC est chargé d'identifier les applications pour une navigation sécurisée. Parmi les critères, le moteur AVC analysera le corps de la réponse pour détecter une application de recherche. Par conséquent, l'appliance ne transférera pas les en-têtes de plage.
- Dans les listes des types d'application, le résumé de chaque type d'application répertorie les actions finales pour ses applications, mais n'indique pas si ces actions sont héritées de la politique globale ou configurées dans la politique d'accès actuelle. Pour en savoir plus sur l'action pour une application particulière, développez le type d'application.
- Dans la politique d'accès globale, vous pouvez définir l'action par défaut pour chaque type d'application, de sorte que les nouvelles applications introduites dans une mise à jour du moteur AVC héritent automatiquement de l'action par défaut.
- Vous pouvez configurer rapidement la même action pour toutes les applications d'un type d'application en cliquant sur le lien « edit all » (modifier tout) correspondant au type d'application dans la vue Browse (Parcourir). Cependant, vous pouvez uniquement configurer l'action de l'application, pas les actions de comportement de l'application. Pour configurer les comportements des applications, vous devez modifier chaque application individuellement.

- Dans la vue de recherche, lorsque vous triez le tableau en fonction de la colonne d'actions, l'ordre de tri est défini par l'action finale. Par exemple, « Use Global (Block) » [Utiliser global (Bloquer)] vient après « Block » (Bloquer) dans l'ordre de tri.
- Le déchiffrement peut faire échouer certaines applications, sauf si le certificat racine de signature est installé sur le client.

Thèmes connexes

- Configuration des paramètres de contrôle des applications dans un groupe de politiques d'accès, on page 352
- Configuration des limites globales de bande passante, on page 353
- Affichage de l'activité AVC , on page 356

Configuration des paramètres de contrôle des applications dans un groupe de politiques d'accès

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans le tableau Policies (Politiques), sous la colonne Applications du groupe de politiques que vous souhaitez modifier.

Étape 3 Lors de la configuration de la politique d'accès globale :

a) Définissez l'action par défaut pour chaque type d'application dans la section **Default Actions for Application Types** (Actions par défaut pour les types d'application).

b) Vous pouvez modifier les actions par défaut pour les membres individuels de chaque type d'application, en tant que groupe ou individuellement, dans la section **Edit Applications Settings** (Modifier les paramètres des applications) de la page. La modification de l'action par défaut pour les applications individuelles est décrite dans les étapes suivantes.

Étape 4 Lors de la configuration d'une politique d'accès définie par l'utilisateur, choisissez **Define Applications Custom Settings** (Définir les paramètres personnalisés des applications) dans la section **Edit Applications Settings** (Modifier les paramètres des applications).

Étape 5 Dans la zone Application Settings (Paramètres des applications), choisissez **Browse view** (Vue Parcourir) ou **Search view** (Vue Rechercher) dans le menu déroulant :

- **Browse view** (Vue Parcourir). Vous pouvez parcourir les types d'application. Vous pouvez utiliser la fonction Browse view (Vue Parcourir) pour configurer simultanément toutes les applications d'un type particulier. Lorsqu'un type d'application est réduit dans la vue Browse (Parcourir), le résumé des types d'application répertorie les actions finales pour ses applications; cependant, il n'indique pas si les actions sont héritées de la politique globale ou configurées dans la politique d'accès actuelle.
- **Search view** (Vue Rechercher). Vous pouvez rechercher des applications par leur nom. Vous pouvez utiliser le mode Search (Rechercher) lorsque la liste totale des applications est longue et que vous devez trouver et configurer rapidement une application particulière.

Étape 6 Configurez l'action pour chaque application et le comportement de l'application.

Étape 7 Configurez les contrôles de bande passante pour chaque application applicable.

Étape 8 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Contrôle de la bande passante, on page 353

Contrôle de la bande passante

Lorsque la limite globale et la limite d'utilisateurs s'appliquent à une transaction, l'option la plus restrictive s'applique. Vous pouvez définir les limites de bande passante pour des catégories d'URL particulières en définissant un groupe d'identité pour une catégorie d'URL et en l'utilisant dans une politique d'accès qui restreint la bande passante.

Vous pouvez définir les limites de bande passante suivantes :

Limite de bande passante	Description	Lien vers la tâche
Overall (Globale)	Définissez une limite globale pour tous les utilisateurs du réseau pour les types d'applications pris en charge. La limite de bande passante globale affecte le trafic entre les serveurs de Secure Web Appliance et d'applications. Elle ne limite pas le trafic diffusé à partir du cache Web.	Configuration des limites globales de bande passante, on page 353
User (Utilisateur)	Définissez une limite pour le nombre d'utilisateurs particuliers sur le réseau par type d'application. La bande passante utilisateur limite le trafic provenant des serveurs Web ainsi que le trafic desservi à partir du cache Web.	Configuration des limites de bande passante pour les utilisateurs, on page 354

Note La définition des limites de bande passante ne limite que les données envoyées aux utilisateurs. Elle ne bloque pas les données en fonction de l'atteinte d'un quota. Le proxy Web introduit une latence dans chaque transaction d'application pour imiter une liaison plus lente avec le serveur.

Configuration des limites globales de bande passante

Étape 1 Choisissez **Web Security Manager > Overall Bandwidth Limits** (Web Security Manager > Limites de bande passante globales).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez l'option **Limit to** (Limiter à).

Étape 4 Saisissez la quantité de trafic à limiter en mégabits par seconde (Mbit/s) ou en kilobits par seconde (kbit/s).

Étape 5 Envoyez et validez les modifications.

Configuration des limites de bande passante pour les utilisateurs

Vous pouvez définir les limites de bande passante utilisateur en configurant les paramètres de contrôle de bande passante dans la page Applications Visibility and Control (Visibilité et contrôle des applications) des politiques d'accès. Vous pouvez définir les types suivants de contrôle de bande passante pour les utilisateurs dans les politiques d'accès :

Option	Description	Lien vers la tâche
Default bandwidth limit for an application type (Limite de bande passante par défaut pour un type d'application)	Dans la politique d'accès globale, vous pouvez définir la limite de bande passante par défaut pour toutes les applications d'un type particulier.	Configuration de la limite de bande passante par défaut pour un type d'application, on page 354
Bandwidth limit for an application type (Limite de bande passante pour un type d'application)	Dans une politique d'accès définie par l'utilisateur, vous pouvez remplacer la limite de bande passante par défaut pour le type d'application défini dans la politique d'accès globale.	Remplacement de la limite de bande passante par défaut pour un type d'application, on page 354
Bandwidth limit for an application (Limite de bande passante pour une application)	Dans une politique d'accès définie ou globale, vous pouvez choisir d'appliquer la limite de bande passante du type d'application ou aucune limite (dispensé de limite selon le type d'application).	Configuration des contrôles de bande passante pour une application, on page 355

Configuration de la limite de bande passante par défaut pour un type d'application

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans le tableau des politiques, sous la colonne Applications pour la politique d'accès globale.

Étape 3 Dans la section **Default Actions for Application Types** (Actions par défaut pour les types d'applications), cliquez sur le lien à côté de « Bandwidth Limit » (Limites de bande passante) pour le type d'application que vous souhaitez modifier.

Étape 4 Sélectionnez **Set Bandwidth Limit** (Définir la limite de bande passante) et saisissez la quantité de trafic à limiter en mégabits par seconde (Mbit/s) ou en kilobits par seconde (kbit/s).

Étape 5 Cliquez sur **Apply** (Appliquer).

Étape 6 Envoyez et validez les modifications.

Remplacement de la limite de bande passante par défaut pour un type d'application

Vous pouvez remplacer la limite de bande passante par défaut définie au niveau du groupe de politiques d'accès globales dans les politiques d'accès définies par l'utilisateur. Vous ne pouvez faire cela que dans la vue Browse (Parcourir).

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Dans le tableau des politiques, sous la colonne Applications, cliquez sur le lien correspondant au groupe de politiques défini par l'utilisateur que vous souhaitez modifier.

Étape 3 Choisissez **Define Applications Custom Settings** (Définir les paramètres personnalisés des applications) dans la section **Edit Applications Settings** (Modifier les paramètres des applications).

Étape 4 Cliquez sur le lien à côté de « Bandwidth Limit » (Limites de bande passante) pour le type d'application que vous souhaitez modifier.

Étape 5 Pour choisir une valeur de limite de bande passante différente, sélectionnez **Set Bandwidth Limit** (Définir la limite de bande passante) et saisissez la quantité de trafic à limiter en mégabits par seconde (Mbit/s) ou en kilobits par seconde (kbit/s). Pour n'indiquer aucune limite de bande passante, sélectionnez **No Bandwidth Limit for Application Type** (Aucune limite de bande passante pour le type d'application).

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 Envoyez et validez les modifications.

Configuration des contrôles de bande passante pour une application

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans le tableau des politiques, sous la colonne Applications, pour le groupe de politiques que vous souhaitez modifier.

Étape 3 Développez le champ du type d'application qui contient l'application à définir.

Étape 4 Cliquez sur le lien de l'application que vous souhaitez configurer.

Étape 5 Sélectionnez **Monitor** (Superviser), puis choisissez d'utiliser la limite de bande passante définie pour le type d'application ou aucune limite.

Note Le paramètre de limite de bande passante n'est pas applicable lorsque l'application est bloquée ou lorsqu'aucune limite de bande passante n'est définie pour le type d'application.

Étape 6 Cliquez sur **Done** (Terminé).

Étape 7 Envoyez et validez les modifications.

Contrôle du trafic de la messagerie instantanée

Vous pouvez bloquer ou surveiller le trafic de messagerie instantanée et selon le service de messagerie instantanée utilisé, vous pouvez bloquer des activités particulières (également appelées comportements d'application) dans une session de messagerie instantanée.

Étape 1 Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans le tableau des politiques, sous la colonne Applications, pour le groupe de politiques que vous souhaitez modifier.

Étape 3 Cliquez sur **Define Applications Custom Setting** (Définir les paramètres personnalisés des applications).

Étape 4 Développez le type d'application de messagerie instantanée.

Étape 5 Cliquez sur le lien à côté de l'application de messagerie instantanée que vous souhaitez configurer.

Étape 6 Pour bloquer tout le trafic pour cette application de messagerie instantanée, sélectionnez **Block** (Bloquer).

Étape 7 Pour surperviser l'application de messagerie instantanée, mais bloquer des activités particulières au sein de l'application, sélectionnez **Monitor** (Superviser), puis sélectionnez **Block** (Bloquer) pour le comportement de l'application.

Étape 8 Cliquez sur **Done** (Terminé).

Étape 9 Envoyez et validez les modifications.

Affichage de l'activité AVC

La page **Reporting > Application Visibility** (Rapports > Visibilité des applications) affiche des informations sur les principales applications et les types d'applications utilisés. Elle affiche également les principales applications et les types d'applications bloquées.

Informations AVC dans le fichier journal d'accès

Le fichier journal des accès enregistre les informations renvoyées par le moteur AVC pour chaque transaction. La section des informations sur le verdict d'analyse dans les journaux d'accès comprend les champs ci-dessous :

Description	Champ personnalisé dans les journaux d'accès	Champ personnalisé dans les journaux W3C
Nom de l'application	%XO	x-avc-app
Type d'application	%Xu	x-avc-type
Comportement des applications	%Xb	x-avc-behavior

CHAPITRE 16

Prévenir la perte de données sensibles

Cette rubrique contient les sections suivantes :

Survol de la prévention de la perte de données sensibles

Secure Web Appliance protège vos données en vous fournissant les fonctionnalités suivantes :

Option	Description
Cisco Data Security filters (Filtres de sécurité des données Cisco)	Les filtres de sécurité des données Cisco sur Secure Web Appliance évaluent les données quittant le réseau sur HTTP, HTTPS et FTP.
Third-party data loss prevention (DLP) integration (Intégration de la protection contre la perte de données par des tiers)	Secure Web Appliance s'intègre aux principaux systèmes de DLP tiers conscients du contenu qui cernent et protègent les données sensibles. Le proxy Web utilise le protocole ICAP (Internet Content Adaptation Protocol), qui permet aux serveurs proxy de décharger l'analyse de contenu vers des systèmes externes.

Lorsque le proxy Web reçoit une demande de téléchargement, il la compare aux groupes de politiques de sécurité des données et de politique de protection contre la perte de données externe pour déterminer le groupe de politiques à appliquer. Si les deux types de politique sont configurés, la demande est comparée aux politiques de sécurité des données Cisco avant les politiques de DLP externes. Après avoir affecté la demande à un groupe de politiques, il compare la demande aux paramètres de contrôle configurés du groupe de politiques pour déterminer la marche à suivre de la demande. La façon dont vous configurez l'appliance pour gérer les demandes de téléchargement dépend du type de groupe de politiques.

Note Les requêtes de chargement qui tentent de charger des fichiers d'une taille de zéro (0) octet ne sont pas évaluées par rapport aux politiques de sécurité des données de Cisco ou de DLP externes.

Pour restreindre et contrôler les données qui quittent le réseau, vous pouvez effectuer les tâches suivantes :

Tâche	Lien vers la tâche
Créer des politiques de sécurité des données de Cisco	Gestion des demandes de chargement, on page 359
Créer des politiques DLP externes	Gestion des demandes de chargement sur un système DLP externes, on page 360
Créer des politiques de sécurité des données et de DLP externe	Création de politiques de sécurité des données et de DLP externes, on page 361
Contrôler les demandes de téléchargement à l'aide des politiques de sécurité des données de Cisco	Gestion des paramètres des demandes de chargement, on page 364
Contrôler les demandes de téléchargement à l'aide de politiques DLP externes	Contrôle des demandes de chargement à l'aide de politiques DLP externes, on page 368

Contournement des demandes de chargement en dessous d'une taille minimale

Pour aider à réduire le nombre de demandes de téléchargement enregistrées dans les fichiers journaux, vous pouvez définir une taille minimale de corps de demande en dessous de laquelle les demandes de téléchargement ne sont pas analysées par les filtres de sécurité des données Cisco ou le serveur DLP externe.

Pour ce faire, utilisez les commandes d'interface de ligne de commande suivantes :

- `datasecurityconfig`. S'applique aux filtres de sécurité des données Cisco.
- `externaldlpconfig`. S'applique aux serveurs DLP externes configurés.

La taille minimale du corps de la demande par défaut est de 4 Ko (4 096 octets) pour les deux commandes d'interface de ligne de commande. Les valeurs correctes sont comprises entre 1 et 64 Ko. La taille que vous spécifiez s'applique à la taille entière du corps de la demande de téléchargement.

Note Tous les chargements codés de blocs et toutes les transactions FTP natives sont analysés par les filtres de sécurité des données de Cisco ou les serveurs DLP externes lorsqu'ils sont activés. Cependant, elles peuvent toujours être contournées en fonction d'une catégorie d'URL personnalisée.

Expérience de l'utilisateur lorsque des demandes sont bloquées en tant que données sensibles

Lorsque des filtres de sécurité des données Cisco ou qu'un serveur DLP externe bloque une demande de chargement, le proxy Web envoie une page de blocage à l'utilisateur final. Tous les sites Web n'affichent pas la page de blocage à l'utilisateur final. Par exemple, certains sites Web 2.0 affichent un contenu dynamique

utilisant javascript au lieu d'une page Web statique et n'afficheront probablement pas la page de blocage. Les utilisateurs sont toujours correctement empêchés de commettre des violations de la sécurité des données, mais ils n'en sont pas toujours informés par le site Web.

Gestion des demandes de chargement

Before you begin

Accédez à **Security Services > Data Security Filters** (Services de sécurité > Filtres de sécurité des données) pour activer les filtres de sécurité des données de Cisco.

Créer et configurer des groupes de politiques de sécurité des données.

Les politiques de sécurité des données de Cisco utilisent le filtrage d'URL, la réputation des sites Web et des informations sur le contenu du téléchargement lors de l'évaluation de la demande de téléchargement. Vous configurez chacun de ces composants de sécurité pour déterminer s'il faut ou non bloquer la demande de téléchargement.

Lorsque le proxy Web compare une demande de téléchargement aux paramètres de contrôle, il évalue les paramètres dans l'ordre. Chaque paramètre de contrôle peut être configuré pour effectuer l'une des actions suivantes pour les politiques de sécurité des données de Cisco :

Action	Description
Block (Bloquer)	Le proxy Web n'autorise pas la connexion et affiche plutôt une page de notification à l'utilisateur final expliquant le motif du blocage.
Allow (Autoriser)	Le proxy Web contourne le reste de l'analyse du service de sécurité de la politique de sécurité des données, puis évalue la demande en fonction des politiques d'accès avant de prendre une action finale. Pour les politiques de sécurité des données de Cisco, l'autorisation contourne le reste de l'analyse de sécurité des données, mais ne contourne pas la DLP externe ou l'analyse de la politique d'accès. La mesure finale que le proxy Web entreprend sur la demande est déterminée par la politique d'accès applicable (ou une politique DLP externe applicable qui peut bloquer la demande).
Monitor (Superviser)	Le proxy Web continue de comparer la transaction aux autres paramètres de contrôle de groupe de la politique de sécurité des données pour déterminer s'il faut bloquer la transaction ou l'évaluer par rapport aux politiques d'accès.

Pour les politiques de sécurité des données de Cisco, seule l'action de blocage est une action finale que le proxy Web exécute sur une demande d'un client. Les actions Monitor (Superviser) et Allow (Autoriser) sont des actions intermédiaires. Dans les deux cas, le proxy Web évalue la transaction par rapport aux politiques DLP externes (si configurées) et aux politiques d'accès. Le proxy Web détermine l'action finale à appliquer en fonction des paramètres de contrôle de groupe de la politique d'accès (ou d'une politique DLP externe applicable qui peut bloquer la demande).

What to do next

Thèmes connexes

- Gestion des demandes de chargement sur un système DLP externes, on page 360

• Gestion des paramètres des demandes de chargement, on page 364

Gestion des demandes de chargement sur un système DLP externes

Pour configurer Secure Web Appliance afin de gérer les demandes de téléchargement sur un système DLP externe, effectuez les tâches suivantes :

Étape 1 Choisissez **Network > External DLP Servers** (Réseau > Serveurs DLP externes). Définissez un système DLP externe. Pour transmettre une demande de téléchargement à un système DLP externe à des fins d'analyse, vous devez définir au moins un système DLP conforme à ICAP sur Secure Web Appliance.

Étape 2 **Créez et configurez les groupes de politiques DLP externes.** Une fois un système DLP externe défini, vous créez et configurez des groupes de politiques DLP externes pour déterminer quelles demandes de téléchargement envoyer au système DLP pour l'analyse.

Étape 3 Lorsqu'une demande de téléchargement correspond à une politique DLP externe, le proxy Web envoie la demande de téléchargement au système DLP en utilisant le protocole ICAP (Internet Content Adaptation Protocol) pour l'analyse. Le système DLP analyse le contenu du corps de la demande et renvoie un verdict de blocage ou d'autorisation au proxy Web. Le verdict Allow (Autorisation) est similaire à l'action Allow (Autorisation) pour les politiques de sécurité des données de Cisco, en ce que la demande de téléchargement sera comparée aux politiques d'accès. La mesure finale que le proxy Web entreprend sur la demande est déterminée par la politique d'accès applicable.

What to do next

Thèmes connexes

• Contrôle des demandes de chargement à l'aide de politiques DLP externes, on page 368
• Définition des systèmes DLP externes, on page 366

Évaluation de l'appartenance aux groupes de politiques de sécurité des données et DLP externes

Chaque demande de client est affectée à une identité, puis évaluée par rapport aux autres types de politiques afin de déterminer à quel groupe de politiques elle appartient selon chaque type. Le proxy Web évalue les *demandes de chargement* par rapport aux politiques de sécurité des données et de DLP externe. Le proxy Web applique les paramètres de contrôle de politiques configurés à une demande d'un client en fonction de l'appartenance au groupe de politiques de la demande du client.

Mise en correspondance des demandes des clients auprès des groupes de politiques de sécurité des données et de DLP externes

Pour déterminer le groupe de politiques auquel une demande d'un client correspond, le proxy Web suit un processus précis pour la mise en correspondance des critères d'appartenance au groupe. Il prend en compte les facteurs suivants pour l'appartenance à un groupe :

- **Identity** (Identité). Chaque demande de client correspond à un profil d'identification, échoue à l'authentification et obtient l'accès invité ou échoue à l'authentification et est résiliée.
- **Authorized users** (Utilisateurs autorisés). Si le profil d'identification affecté nécessite une authentification, l'utilisateur doit figurer dans la liste des utilisateurs autorisés dans le groupe de sécurité des données ou de politique DLP externe pour correspondre au groupe de politiques. La liste des utilisateurs autorisés peut comprendre n'importe quel groupe ou utilisateur spécifié ou peut être des utilisateurs invités si le profil d'identification permet l'accès comme invité.
- **Advanced options** (Options avancées). Vous pouvez configurer plusieurs options avancées pour l'appartenance aux groupes de sécurité des données et de politiques DLP externes. Certaines options (telles que le port proxy et la catégorie d'URL) peuvent également être définies dans la section Identity (Identité). Lorsqu'une option avancée est configurée dans la section Identity (Identité), elle n'est pas configurable au niveau du groupe de sécurité des données ou des politiques DLP externes.

Les informations contenues dans cette section donnent un aperçu de la façon dont le proxy Web fait correspondre les demandes de chargement aux groupes de sécurité des données et aux groupes de politiques DLP externes.

Le proxy Web lit successivement chaque groupe de politiques dans le tableau des politiques. Il compare l'état de la demande de chargement aux critères d'appartenance du premier groupe de politiques. S'ils correspondent, le proxy Web applique les paramètres de politique de ce groupe de politiques.

S'ils ne correspondent pas, le proxy Web compare la demande de chargement au groupe de politiques suivant. Il poursuit ce processus jusqu'à ce qu'il fasse correspondre la demande de chargement à un groupe de politiques défini par l'utilisateur. S'il ne correspond pas à un groupe de politiques défini par l'utilisateur, il correspond au groupe de politiques global. Lorsque le proxy Web fait correspondre la demande de chargement à un groupe de politiques ou au groupe de politiques global, il applique les paramètres de politiques de ce groupe de politiques.

Création de politiques de sécurité des données et de DLP externes

Vous pouvez créer des groupes de politiques de sécurité des données et de DLP externes en fonction de combinaisons de plusieurs critères, comme un ou plusieurs profils d'identification ou la catégorie d'URL du site de destination. Vous devez définir au moins un critère d'appartenance à un groupe de politiques. Lorsque vous définissez plusieurs critères, la demande de chargement doit satisfaire à tous les critères pour correspondre au groupe de politiques. Cependant, la demande de téléchargement ne doit correspondre qu'à un des profils d'identification configurés.

Étape 1 Choisissez **Web Security Manager > Cisco Data Security** (Web Security Manager > Politiques de sécurité des données de Cisco) (pour la définition de l'appartenance au groupe de politiques de sécurité des données) ou **Web Security Manager > External Data Loss Prevention** (Web Security Manager > Prévention de la perte de données externe) (pour la définition de l'appartenance au groupe de politiques DLP externes).

Étape 2 Cliquez sur **Add Policy** (Ajouter une politique).

Étape 3 Dans le champ **Policy Name** (Nom de la politique), saisissez le nom du groupe de politiques et dans le champ Description (facultatif), ajoutez une description.

Note Chaque nom de groupe de politiques doit être unique et contenir uniquement des caractères alphanumériques ou un espace.

Étape 4 Dans le champ **Insert Above Policy** (Insérer au-dessus de la politique), choisissez l'emplacement du tableau des politiques où placer le groupe de politiques.

Lors de la configuration de plusieurs groupes de politiques, vous devez préciser un ordre logique pour chaque groupe. Ordonnez vos groupes de politiques pour vous assurer d'une mise en correspondance correcte.

Étape 5 Dans la section **Identity and Users** (Identités et utilisateurs), choisissez un ou plusieurs groupes de profils d'identification à appliquer à ce groupe de politiques.

Étape 6 (Facultatif) Développez la section **Advanced** (Niveau avancé) pour définir les exigences d'appartenance supplémentaires.

Étape 7 Pour définir l'appartenance à un groupe de politiques en fonction des options avancées, cliquez sur le lien de l'option avancée et configurez l'option dans la page qui s'affiche.

Option avancée	Description
Protocols (Protocoles)	Choisissez de définir ou non l'appartenance au groupe de politiques par le protocole utilisé dans la demande du client. Sélectionnez les protocoles à inclure. « All others » (Tous les autres) désigne tout protocole non répertorié au-dessus de cette option. **Note** Lorsque le proxy HTTPS est activé, seules les politiques de déchiffrement s'appliquent aux transactions HTTPS. Vous ne pouvez pas définir l'appartenance aux politiques à l'aide du protocole HTTPS pour les politiques d'accès, de routage, d'analyse des programmes malveillants sortants, de sécurité des données ou DLP externes.
Proxy Ports (Ports du proxy)	Choisissez de définir ou non l'appartenance au groupe de politiques par le port de proxy utilisé pour accéder au proxy Web. Entrez un ou plusieurs numéros de port dans le champ Proxy Ports (Ports du proxy). Séparez les valeurs de ports multiples par des virgules. Pour les connexions de transfert explicite, il s'agit du port configuré dans le navigateur. Pour les connexions transparentes, il s'agit du même port de destination. Vous pouvez définir l'appartenance à un groupe de politiques sur le port du proxy, si un ensemble de clients est configuré pour transférer explicitement les demandes sur un port et un autre ensemble de clients est configuré pour transférer explicitement les demandes sur un port différent. Cisco recommande de définir l'appartenance au groupe de politiques par le port proxy uniquement lorsque l'appliance est déployée en mode de transfert explicite ou lorsque les clients transfèrent explicitement les demandes à l'appliance. Si vous définissez l'appartenance à un groupe de politiques par le port proxy lorsque les demandes des clients sont redirigées de manière transparente vers l'appliance, certaines demandes peuvent être refusées. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques autre que l'identité.

Option avancée	Description
Subnets (Sous-réseaux)	Choisissez de définir ou non l'appartenance au groupe de politiques par sous-réseau ou autres adresses. Vous pouvez choisir d'utiliser les adresses qui peuvent être définies avec le profil d'identification connexe, ou vous pouvez entrer des adresses spécifiques ici. **Note** Si le profil d'identification associé à ce groupe de politiques définit ses membres par des adresses, dans ce groupe de politiques, vous devez saisir des adresses qui constituent un sous-ensemble des adresses définies dans le profil d'identification. L'ajout d'adresses dans le groupe de politiques réduit davantage la liste des transactions qui correspondent à ce groupe de politiques.
URL Categories (Catégories d'URL)	Choisissez de définir ou non l'appartenance au groupe de politiques par catégories d'URL. Sélectionnez les catégories d'URL prédéfinies ou définies par l'utilisateur. **Note** Si l'identité associée à ce groupe de politiques définit l'appartenance à l'identité par ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques autre que l'identité.
User Agents (Agents utilisateur)	Choisissez si vous souhaitez définir l'appartenance au groupe de politiques en fonction des agents utilisateur (applications clientes telles que les programmes de mise à jour et les navigateurs Web) utilisés dans la demande du client. Vous pouvez sélectionner des agents utilisateur couramment définis ou définir les vôtres à l'aide d'expressions régulières. Indique si la définition d'appartenance inclut uniquement les agents utilisateur sélectionnés ou exclut expressément les agents utilisateur sélectionnés. **Note** Si le profil d'identification associé à ce groupe de politiques définit l'appartenance au profil d'identification en fonction de ce paramètre avancé, le paramètre ne peut pas être configuré au niveau du groupe de politiques sans profil d'identification.
User Location (Emplacement de l'utilisateur)	Choisissez de définir ou non l'appartenance au groupe de politiques par emplacement d'utilisateur, distant ou local. Cette option ne s'affiche que lorsque la solution Secure Mobility est activée.

Étape 8 Envoyez vos modifications.

Étape 9 Si vous créez un groupe de politique de sécurité des données, configurez ses paramètres de contrôle pour définir comment le proxy Web gère les demandes de téléchargement.

Le nouveau groupe de politiques de sécurité des données hérite automatiquement des paramètres globaux du groupe de politiques jusqu'à ce que vous configuriez des options pour chaque paramètre de contrôle.

Si vous créez un groupe de politiques de DLP externe, configurez ses paramètres de contrôle pour définir comment le proxy Web gère les demandes de téléchargement.

Le nouveau groupe de politiques DLP externe hérite automatiquement des paramètres globaux du groupe de politiques jusqu'à ce que vous configuriez des paramètres personnalisés.

Étape 10 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Évaluation de l'appartenance aux groupes de politiques de sécurité des données et DLP externes, on page 360
- Mise en correspondance des demandes des clients auprès des groupes de politiques de sécurité des données et de DLP externes, on page 361
- Gestion des paramètres des demandes de chargement, on page 364
- Contrôle des demandes de chargement à l'aide de politiques DLP externes, on page 368

Gestion des paramètres des demandes de chargement

Chaque demande de chargement est affectée à un groupe de politiques de sécurité des données et hérite des paramètres de contrôle de ce groupe de politiques. Les paramètres de contrôle du groupe de politiques de sécurité des données déterminent si l'appliance bloque la connexion ou l'évalue en fonction des politiques d'accès.

Configurez les paramètres de contrôle des groupes de politiques de sécurité des données sur la page Web Security Manager > Cisco Data Security.

Vous pouvez configurer les paramètres suivants pour déterminer les mesures à prendre concernant les demandes de chargement :

Option	Lien
URL Categories (Catégories d'URL)	URL Categories (Catégories d'URL), on page 364
Web Reputation (Réputation Web)	Réputation Web, on page 364
Content (Contenu)	Blocage de contenu, on page 365

Après l'affectation d'un groupe de politiques de sécurité des données à une demande de chargement, les paramètres de contrôle du groupe de politiques sont évalués afin de déterminer s'il faut bloquer la demande ou l'évaluer par rapport aux politiques d'accès.

URL Categories (Catégories d'URL)

AsyncOS pour le Web vous permet de configurer la façon dont l'appliance traite une transaction en fonction de la catégorie d'URL d'une demande particulière. À l'aide d'une liste de catégories prédéfinies, vous pouvez choisir de surveiller ou de bloquer le contenu par catégorie. Vous pouvez également créer des catégories d'URL personnalisées et choisir d'autoriser, de surveiller ou de bloquer le trafic pour un site Web dans la catégorie personnalisée.

Réputation Web

Le paramètre de réputation Web hérite du paramètre global. Pour personnaliser le filtrage de réputation Web pour un groupe de politiques particulier, vous pouvez utiliser le menu déroulant Web Reputation Settings (Paramètres de réputation Web) afin de personnaliser les seuils de score de réputation Web.

Seules des valeurs négatives et nulles peuvent être configurées pour les paramètres de seuil de réputation Web pour les politiques de sécurité des données de Cisco. Par définition, toutes les évaluations positives sont surveillées.

Blocage de contenu

Vous pouvez utiliser les paramètres de la page Cisco Data Security > Content (Sécurité des données Cisco > Contenu) pour configurer le proxy Web de manière à bloquer les chargements de données en fonction des caractéristiques de fichier suivantes :

- **File size** (Taille du fichier). Vous pouvez préciser la taille maximale de *chargement* autorisée. Tous les chargements dont la taille est égale ou supérieure au maximum spécifié sont bloqués. Vous pouvez spécifier des tailles de fichier maximales différentes pour les demandes HTTP/HTTPS et FTP natives.

  Lorsque la taille de la demande de chargement est supérieure à la taille de chargement maximale et à la taille d'analyse maximale (configurées dans le champ « DVS Engine Object Scanning Limits » [Limites d'analyse d'objet du moteur DVS) sur la page Security Services > Anti-Malware (Services de sécurité > Protection contre les programmes malveillants)], la demande de chargement est toujours bloquée, mais l'entrée dans les journaux de sécurité des données n'enregistre pas le nom du fichier et le type de contenu. L'entrée dans les journaux d'accès reste inchangée.

- **File type** (Type de fichier). Vous pouvez bloquer les types de fichiers prédéfinis ou les types MIME personnalisés que vous saisissez. Lorsque vous bloquez un type de fichier prédéfini, vous pouvez bloquer tous les fichiers de ce type ou les fichiers supérieurs à la taille spécifiée. Lorsque vous bloquez un type de fichier en fonction de la taille, la taille maximale de fichier que vous pouvez spécifier est identique à la valeur du champ « DVS Engine Object Scanning Limits » (Limites d'analyse des objets du moteur DVS) sur la page Security Services > Anti-Malware (Services de sécurité > Antiprogrammes malveillants). Par défaut, cette valeur est de 32 Mo.

  Les filtres de sécurité des données Cisco n'inspectent pas le contenu des fichiers archivés lors du blocage par type de fichier. Les fichiers archivés peuvent être bloqués par leur type de fichier ou par le nom de fichier, et non en fonction de leur contenu.

Note Pour certains groupes de types MIME, le blocage d'un type bloque tous les types MIME du groupe. Par exemple, le blocage de application/x-java-Applet bloque tous les types MIME java, tels que application/java et application/javascript.

- **File name** (Nom de fichier). Vous pouvez bloquer des fichiers portant des noms spécifiques. Vous pouvez utiliser text comme chaîne littérale ou expression régulière pour préciser les noms de fichiers à bloquer.

Note Saisissez uniquement des noms de fichiers comprenant des caractères ASCII 8 bits. Le proxy Web ne met en correspondance que les noms de fichiers contenant des caractères ASCII 8 bits.

Définition des systèmes DLP externes

Secure Web Appliance peut s'intégrer à plusieurs serveurs DLP externes du même fournisseur en définissant plusieurs serveurs DLP dans l'appliance. Vous pouvez définir la technique d'équilibrage de la charge que le proxy Web utilise lorsqu'il communique avec les systèmes DLP. Cela est utile lorsque vous définissez plusieurs systèmes DLP. Consultez Configuration SSL , on page 606 pour en savoir plus sur la spécification des protocoles utilisés pour sécuriser les communications avec les serveurs DLP externes.

Note Vérifiez que le serveur DLP externe n'envoie pas le contenu modifié du proxy Web. AsyncOS pour le Web prend uniquement en charge la possibilité de bloquer ou d'autoriser les demandes de téléchargement. Il ne prend pas en charge le téléchargement de contenu modifié par un serveur DLP externe.

Configuration des serveurs DLP externes

Étape 1 Choisissez **Network > External DLP Servers** (Réseau > Serveurs DLP externes).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Paramètres	Description
Protocol for External DLP Servers (Protocole pour les serveurs DLP externes)	Choisissez l'un des paramètres suivants : • **ICAP** : les communications ICAP client/serveur DLP ne sont pas chiffrées. • **Secure ICAP** (ICAP sécurisé) : les communications ICAP client/serveur DLP se font par un tunnel chiffré. D'autres options connexes s'affichent.

Paramètres	Description
External DLP Servers (Serveurs DLP externes)	Saisissez les informations suivantes pour accéder à un système DLP conforme à ICAP : • **Server address** (Adresse du serveur) et **Port** : nom d'hôte ou adresse IP et port TCP pour accéder au système DLP. • **Reconnection attempts** (Tentatives de reconnexion) : nombre de fois que le proxy Web tente de se connecter au système DLP avant d'échouer. • **Service URL** (URL du service) : URL de requête ICAP spécifique au serveur DLP en question. Le proxy Web inclut les informations que vous saisissez ici dans la demande ICAP envoyée au serveur DLP externe. L'URL doit commencer par le protocole ICAP : icap:// • Certificate (Certificat) (facultatif) : le certificat fourni pour sécuriser chaque connexion au serveur DLP externe peut être signé par l'autorité de certification (AC) ou autosigné. Obtenez le certificat du serveur spécifié, puis chargez-le sur l'appliance : • Recherchez et sélectionnez le fichier de certificat, puis cliquez sur **Upload File** (Charger le fichier). **Note** Ce fichier unique doit contenir le certificat client et la clé privée au format non chiffré. • **Use this certificate for all DLP server using Secure ICAP** (Utiliser ce certificat pour tous les serveurs DLP utilisant Secure ICAP) : cochez cette case pour utiliser le même certificat pour tous les serveurs DLP externes que vous définissez ici. Laissez l'option décochée pour saisir un certificat différent pour chaque serveur. • Start Test (Démarrer le test) : vous pouvez tester la connexion entre Secure Web Appliance et le ou les serveurs DLP externes définis en cliquant sur **Start Test** (Démarrer le test).
Équilibrage de la charge	Si plusieurs serveurs DLP sont définis, sélectionnez la technique d'équilibrage de la charge que le proxy Web utilise pour distribuer les demandes de chargement vers différents serveurs DLP. Vous pouvez choisir les techniques d'équilibrage de la charge suivantes : • **None (failover)** [Aucune (basculement)] Le proxy Web dirige les demandes de téléchargement vers un serveur DLP. Il essaie de se connecter aux serveurs DLP dans l'ordre dans lequel ils sont répertoriés. Si un serveur DLP ne peut pas être atteint, le proxy Web tente de se connecter au suivant dans la liste. • **Fewest connections** (Le moins de connexions possibles). Le proxy Web suit le nombre de demandes actives provenant des différents serveurs DLP et dirige la demande de chargement vers le serveur DLP qui traite actuellement le plus petit nombre de connexions. • **Hash based** (Basé sur le hachage). Le proxy Web utilise une fonction de hachage pour distribuer les demandes aux serveurs DLP. La fonction de hachage utilise l'ID et l'URL du proxy comme entrées de sorte que les demandes pour la même URL soient toujours dirigées vers le même serveur DLP. • **Round robin** (Circuit cyclique). Le proxy Web distribue les demandes de chargement de manière égale sur tous les serveurs DLP dans l'ordre indiqué.

Paramètres	Description
Service Request Timeout (Délai d'expiration des demandes de service)	Entrez le temps pendant lequel le proxy Web attend une réponse du serveur DLP. Lorsque ce délai est dépassé, la demande ICAP échoue et la demande de chargement est soit bloquée, soit autorisée, selon le paramètre de gestion des défaillances. La valeur par défaut est 60 secondes.
Maximum Simultaneous Connections (Nombre maximal de connexions simultanées)	Indique le nombre maximal de connexions de demande ICAP simultanées de Secure Web Appliance vers chaque serveur DLP externe configuré. Le paramètre de gestion des défaillances dans cette page s'applique à toute demande qui dépasse cette limite. La valeur par défaut est 25.
Failure Handling (Gestion des échecs)	Choisissez si les demandes de chargement sont bloquées ou autorisées (transmises aux politiques d'accès pour évaluation) lorsque le serveur DLP ne parvient pas à fournir une réponse rapide. La valeur par défaut est allow (« Permit all data transfers to proceed without scanning ») [allow (« autoriser la poursuite de tous les transferts de données sans analyse »)].
Trusted Root Certificate (Certificat racine approuvé)	Recherchez et sélectionnez le certificat racine approuvé pour les certificats fournis avec les serveurs DLP externes, puis cliquez sur Upload File (Charger le fichier). Voir Certificate Management, on page 608 pour de plus amples informations.
Invalid Certificate Options (Options de certificats non valides)	Indiquez comment les divers certificats non valides sont traités : **Drop** (Supprimer) ou **Monitor** (Superviser).
Server Certificates (Certificats du serveur)	Cette section affiche tous les certificats de serveur DLP actuellement disponibles sur l'appliance.

Étape 3 (Facultatif) Vous pouvez ajouter un autre serveur DLP en cliquant sur **Add Row** (Ajouter une ligne) et en saisissant les informations du serveur DLP dans les nouveaux champs fournis.

Étape 4 Envoyez et validez les modifications.

Contrôle des demandes de chargement à l'aide de politiques DLP externes

Une fois que le proxy Web reçoit les en-têtes de demande de chargement, il dispose des informations nécessaires pour décider si la demande doit être transmise au système DLP externe pour analyse. Le système DLP analyse la demande et renvoie un verdict au proxy Web, à savoir bloquer ou superviser (évaluer la demande par rapport aux politiques d'accès).

Étape 1 Choisissez **Web Security Manager > External Data Loss Prevention** (Web Security Manager > Prévention de la perte de données externes).

Étape 2 Cliquez sur le lien sous la colonne Destinations du groupe de politiques que vous souhaitez configurer.

Étape 3 Dans la section **Edit Destination Settings** (Modifier les paramètres de destination), choisissez « **Define Destinations Scanning Custom Settings** » (Définir les paramètres personnalisés d'analyse des destinations).

Étape 4 Dans la section **Destination to scan** (Destination à analyser), choisissez l'une des options suivantes :

- **Do not scan any uploads** (N'analyser aucun chargement). Aucune demande de chargement n'est envoyée au(x) système(s) DLP configuré(s) pour analyse. Toutes les demandes de chargement sont évaluées par rapport aux politiques d'accès.
- **Scan all uploads** (Analyser tous les chargements) Toutes les demandes de chargement sont envoyées au(x) système(s) DLP configuré(s) pour analyse. La demande de chargement est bloquée ou évaluée par rapport aux politiques d'accès en fonction du verdict émis à l'issue de l'analyse du système DLP.
- **Scan uploads except to specified custom and external URL categories** (Analyser les chargements, sauf dans les catégories d'URL personnalisées et externes spécifiées) Les demandes de chargement qui appartiennent à des catégories d'URL personnalisées spécifiques sont exclues des politiques d'analyse DLP. Cliquez sur **Edit custom categories list** (Modifier la liste des catégories personnalisées) pour sélectionner les catégories d'URL à analyser.

Étape 5 Envoyez et validez les modifications.

Journalisation de l'analyse de prévention de la perte de données

Les journaux d'accès indiquent si une demande de chargement a été analysée par les filtres de sécurité des données Cisco ou par un serveur DLP externe. Les entrées du journal d'accès comprennent un champ pour le verdict de l'analyse de sécurité des données Cisco et un autre champ pour le verdict de l'analyse DLP externe en fonction du verdict.

En plus des journaux d'accès, Secure Web Appliance fournit les types de fichiers journaux suivants pour dépanner la sécurité des données et les politiques DLP externes de Cisco :

- **Data Security Logs** (Journaux de sécurité des données). Enregistre l'historique du client pour les demandes de chargement évaluées par les filtres de sécurité des données Cisco.
- **Data Security Module Logs** (Journaux du module de sécurité des données). Enregistre les messages liés aux filtres de sécurité des données Cisco.
- **Default Proxy Logs** (Journaux de proxy par défaut). En plus d'enregistrer les erreurs liées au proxy Web, les journaux de proxy par défaut incluent les messages relatifs à la connexion aux serveurs DLP externes. Cela vous permet de résoudre les problèmes de connectivité ou d'intégration aux serveurs DLP externes.

Le texte suivant illustre un exemple d'entrée de journal de sécurité des données :

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

Valeur de champ	Description
`Mon Mar 30 03:02:13 2009 Info:`	Horodatage et niveau de suivi
`303`	ID de transaction

Valeur de champ	Description
`10.1.1.1`	Adresse IP source
`-`	Nom d'utilisateur
`-`	Noms de groupes autorisés
`<<bar,text/plain,5120><foo,text/plain,5120>>`	Nom du fichier, type de fichier et taille de chaque fichier chargé simultanément **Note** Ce champ n'inclut pas les fichiers texte ou bruts dont la taille est inférieure à la taille minimale configurée du corps de la demande, dont la valeur par défaut est de 4096 octets.
`BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting`	Politiques et actions de sécurité des données Cisco
`ns`	Niveau de réputation Web
`server.com`	URL sortante
`nc`	Catégorie de l'URL

Note Pour savoir quand le transfert de données, comme une demande POST, vers un site a été bloqué par le serveur DLP externe, recherchez l'adresse IP ou le nom d'hôte du serveur DLP dans les journaux d'accès.

CHAPITRE 17

Aviser les utilisateurs finaux des actions du proxy

Cette rubrique contient les sections suivantes :

Survol des notifications envoyées à l'utilisateur final

Vous pouvez configurer les types de notifications suivants pour les utilisateurs finaux :

Option	Description	Informations complémentaires
Page End-user acknowledgement (Accusé de réception de l'utilisateur final)	Informe les utilisateurs finaux que leur activité Web est filtrée et surveillée. Une page d'accusé de réception de l'utilisateur final s'affiche lorsqu'un utilisateur accède à un navigateur pour la première fois après un certain temps.	page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final), on page 373
Pages End-User Notification (Notification d'utilisateur final)	Page présentée aux utilisateurs finaux lorsque l'accès à une page particulière est bloqué, en fonction du motif du blocage.	Pages End-User Notification (Notification d'utilisateur final) , on page 377

Option	Description	Informations complémentaires
Page End-user URL filtering warning (Avertissement concernant le filtrage d'URL de l'utilisateur final)	Avertit les utilisateurs finaux qu'un site auquel ils accèdent ne respecte pas les politiques d'utilisation acceptable de votre organisation et leur permet de continuer s'ils le choisissent.	Configuration de la page d'avertissement du filtrage des URL de l'utilisateur final, on page 381
FTP notification messages (Messages de notification FTP)	Indique aux utilisateurs finaux le motif du blocage d'une transaction FTP native.	Configuration des messages de notification FTP, on page 382.
Page Time and Volume Quotas Expiry Warning (Avertissement d'expiration des quotas de volume et de temps)	Avertit les utilisateurs finaux lorsque leur accès est bloqué parce qu'ils ont atteint la limite de volume de données ou de temps configurée.	Configurez ces paramètres dans la page d'avertissement d'expiration des quotas de temps et de volume, section Security Services > End User Notification (Services de sécurité > Notification de l'utilisateur final). Voir aussi Plages de temps et quotas, on page 269.

Configuration des paramètres généraux pour les pages de notification

Indiquez les langues d'affichage et le logo des pages de notification. Les restrictions sont décrites dans la présente procédure.

Étape 1 Sélectionnez **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la section des paramètres généraux, sélectionnez la langue que le proxy Web doit utiliser lors de l'affichage des pages de notification.

- Le paramètre de langue HTTP s'applique à toutes les pages de notification HTTP (accusé de réception, utilisateur final sur la boîte, utilisateur final personnalisé et avertissement de filtrage d'URL de l'utilisateur final).
- La langue du FTP s'applique à tous les messages de notification FTP.

Étape 4 Choisissez d'utiliser ou non un logo sur chaque page de notification. Vous pouvez indiquer le logo Cisco ou tout fichier graphique référencé dans l'URL que vous saisissez dans le champ Use Custom Logo (Utiliser un logo personnalisé).

Ce paramètre s'applique à toutes les pages de notification HTTP desservies sur IPv4. AsyncOS ne prend pas en charge les images sur IPv6.

Étape 5 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Mises en garde concernant les URL et les logos dans les pages de notification , on page 383

page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final)

Vous pouvez configurer Secure Web Appliance pour informer les utilisateurs qu'il filtre et surveille leur activité Web. Une fois ce paramètre configuré, l'appliance affiche une page d'accusé de réception de l'utilisateur final pour chaque utilisateur accédant au Web à l'aide de HTTP ou HTTPS. Elle affiche la page d'accusé de réception de l'utilisateur final la première fois qu'un utilisateur tente d'accéder à un site Web ou après un intervalle de temps configuré.

Le proxy Web suit les utilisateurs par nom d'utilisateur si l'authentification a rendu un nom d'utilisateur disponible. Si aucun nom d'utilisateur n'est disponible, vous pouvez choisir votre mode de suivi, par adresse IP ou par témoin de session de navigateur Web.

Note Les transactions FTP natives sont exclues de la page d'accusé de réception de l'utilisateur final.

- Accès aux sites HTTPS et FTP avec la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final), on page 373
- À propos de la page End-user Acknowledgment (Accusé de réception de l'utilisateur final), on page 374
- Configuration de la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final), on page 374

Accès aux sites HTTPS et FTP avec la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final)

La page d'accusé de réception de l'utilisateur final fonctionne, car elle affiche une page HTML à l'utilisateur final qui l'oblige à cliquer sur un contrat de politique d'utilisation acceptable. Une fois que les utilisateurs ont cliqué sur le lien, le proxy Web redirige les clients vers le site Web initialement demandé. Il conserve une trace du moment où les utilisateurs ont accepté la page d'accusé de réception de l'utilisateur final à l'aide d'un remplaçant (par adresse IP ou témoin de session de navigateur Web) si aucun nom d'utilisateur n'est disponible pour l'utilisateur.

- **HTTPS.** Le proxy Web vérifie si l'utilisateur a accusé réception de la page de confirmation de l'utilisateur final à l'aide d'un témoin, mais il ne peut pas obtenir le témoin s'il ne déchiffre pas la transaction. Vous pouvez choisir de contourner (interconnexion) ou d'abandonner les requêtes HTTPS lorsque la page de confirmation de l'utilisateur final est activée et suit les utilisateurs à l'aide de témoins de session. Pour ce faire, utilisez la commande advancedproxyconfig > EUN de l'interface de ligne de commande et choisissez la commande bypass (contourner) pour « Action à exécuter pour les requêtes HTTPS avec EUA basé sur la session (« bypass » ou « drop ») ».
- **FTP sur HTTP.** Les navigateurs Web n'envoient jamais de témoins pour les transactions FTP sur HTTP, de sorte que le proxy Web ne peut pas obtenir de témoin. Pour contourner ce problème, vous pouvez

dispenser les transactions FTP sur HTTP d'exiger la page d'accusé de réception de l'utilisateur final. Pour ce faire, créez une catégorie d'URL personnalisée en utilisant l'expression régulière « ftp:// » comme expression régulière (sans les guillemets) et définissez une politique d'identité qui exonère les utilisateurs de la page de confirmation de l'utilisateur final pour cette catégorie d'URL personnalisée.

À propos de la page End-user Acknowledgment (Accusé de réception de l'utilisateur final)

- Lorsqu'un utilisateur est suivi par son adresse IP, l'appliance utilise la valeur la plus courte pour l'intervalle de temps maximal et le délai d'inactivité maximal de l'adresse IP pour déterminer quand afficher à nouveau la page d'accusé de réception de l'utilisateur final.
- Lorsqu'un utilisateur est suivi à l'aide d'un témoin de session, le proxy Web affiche à nouveau la page d'accusé de réception de l'utilisateur final si l'utilisateur ferme puis rouvre son navigateur Web ou ouvre un deuxième navigateur Web.
- L'utilisation d'un témoin de session pour suivre les utilisateurs lorsque le client accède à des sites HTTPS ou à des serveurs FTP au moyen de FTP sur HTTP ne fonctionne pas.
- Lorsque l'appliance est déployée en mode de transfert explicite et qu'un utilisateur accède à un site HTTPS, la page d'accusé de réception de l'utilisateur final n'inclut que le nom de domaine dans le lien qui redirige l'utilisateur vers l'URL demandée à l'origine. Si l'URL demandée à l'origine contient du texte après le nom de domaine, ce texte est tronqué.
- Lorsque la page d'accusé de réception de l'utilisateur final s'affiche, l'entrée du journal d'accès pour cette transaction indique OTHER (AUTRE) comme balise de décision ACL. En effet, l'URL demandée à l'origine a été bloquée et la page d'accusé de réception de l'utilisateur final a été affichée à la place de l'utilisateur.

Configuration de la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final)

Before you begin

- Pour configurer la langue d'affichage et personnaliser le logo affiché, consultez Configuration des paramètres généraux pour les pages de notification, on page 372.
- Si vous souhaitez personnaliser le message affiché aux utilisateurs finaux, consultez Messages personnalisés sur les pages de notification, on page 382. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 384.

Vous pouvez activer et configurer la page d'accusé de réception de l'utilisateur final dans l'interface Web ou l'interface de ligne de commande. Lorsque vous configurez la page d'accusé de réception de l'utilisateur final dans l'interface Web, vous pouvez inclure un message personnalisé qui s'affiche sur chaque page.

Dans l'interface de ligne de commande, utilisez `advancedproxyconfig` > `eun`.

Étape 1 Choisissez **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez le champ « **Require end-user to click through acknowledgment page** » (Exiger de l'utilisateur final qu'il fasse un clic sur la page d'accusé de réception).

Étape 4 Saisissez des options :

Paramètres	Description
Time Between Acknowledgements (Délai entre les accusés de réception)	L'intervalle entre les accusés de réception détermine la fréquence à laquelle le proxy Web affiche la page d'accusé de réception de l'utilisateur final pour chaque utilisateur. Ce paramètre s'applique aux utilisateurs suivis par nom d'utilisateur et utilisateurs par adresse IP ou témoin de session. Vous pouvez indiquer n'importe quelle valeur comprise entre 30 et 2 678 400 secondes (un mois). La valeur par défaut est un jour (86 400 secondes). Lorsque la durée entre les accusés de réception change et est validée, le proxy Web utilise la nouvelle valeur même pour les utilisateurs qui ont déjà accusé réception du proxy Web.
Inactivity Timeout (Délai d'inactivité maximum)	Le délai d'inactivité détermine combien de temps un utilisateur suivi et reconnu par son adresse IP ou son témoin de session (utilisateurs non authentifiés uniquement) peut être inactif avant que l'utilisateur ne soit plus considéré comme ayant accepté la politique d'utilisation acceptable. Vous pouvez indiquer n'importe quelle valeur comprise entre 30 et 2 678 400 secondes (un mois). La valeur par défaut est de 4 heures (14 400 secondes).

Paramètres	Description
Surrogate Type (Type de substitution)	Détermine la méthode que le proxy Web utilise pour suivre l'utilisateur : • **Adresse IP.** Le proxy Web permet à l'utilisateur de cette adresse IP d'utiliser n'importe quel navigateur Web ou processus HTTP autre qu'un navigateur pour accéder au Web une fois que l'utilisateur a cliqué sur le lien de la page d'accusé de réception de l'utilisateur final. Le suivi de l'utilisateur par adresse IP permet à l'utilisateur d'accéder au Web jusqu'à ce que le proxy Web affiche une nouvelle page d'accusé de réception pour l'utilisateur final en raison de l'inactivité ou de l'intervalle de temps configuré pour les nouveaux accusés de réception. Contrairement au suivi par témoin de session, le suivi par adresse IP permet à l'utilisateur d'ouvrir plusieurs applications de navigateur Web sans avoir à accepter l'accusé de réception de l'utilisateur final, à moins que l'intervalle configuré n'ait expiré. **Note** Lorsque l'adresse IP est configurée et que l'utilisateur est authentifié, le proxy Web suit les utilisateurs par nom d'utilisateur plutôt que par adresse IP. • **Témoin de session.** Le serveur proxy Web envoie un témoin au navigateur Web de l'utilisateur lorsque l'utilisateur cliquez sur le lien de la page d'accusé de réception de l'utilisateur final et utilise le témoin pour suivre sa session. Les utilisateurs peuvent continuer à accéder au Web à l'aide de leur navigateur Web jusqu'à ce que la valeur du Délai entre les accusés de réception expire, ils ont été inactifs plus longtemps que le temps alloué ou ils ferment leur navigateur Web. Si l'utilisateur utilise une application cliente HTTP sans navigateur, il doit être en mesure de cliquer sur le lien sur la page d'accusé de réception de l'utilisateur final pour accéder à Web. Si l'utilisateur ouvre une deuxième application de navigateur Web, l'utilisateur doit exécuter à nouveau le processus d'accusé de réception de l'utilisateur final pour que le proxy Web envoie un témoin de session au deuxième navigateur Web. **Note** L'utilisation d'un témoin de session pour suivre les utilisateurs lorsque le client accède à des sites HTTPS ou à des serveurs FTP au moyen de FTP sur HTTP n'est pas prise en charge.
Custom message (Message personnalisé)	Personnalisez le texte qui s'affiche sur chaque page de confirmation de l'utilisateur final. Vous pouvez inclure des balises HTML simples pour mettre en forme le texte. **Note** Vous ne pouvez inclure un message personnalisé que lorsque vous configurez la page d'accusé de réception de l'utilisateur final dans l'interface Web, plutôt que dans l'interface de ligne de commande. Voir aussi Messages personnalisés sur les pages de notification, on page 382.

Étape 5 (Facultatif) Cliquez sur **Preview Acknowledgment Page Customization** (Survol de la personnalisation de la page d'accusé de réception) pour afficher la page d'accusé de réception actuelle de l'utilisateur final dans une fenêtre de navigateur distincte.

Note Si les fichiers HTML de notification ont été modifiés, cette fonctionnalité d'aperçu n'est pas disponible.

Étape 6 Envoyez et validez les modifications.

Pages End-User Notification (Notification d'utilisateur final)

Lorsqu'une politique empêche un utilisateur d'accéder à un site Web, vous pouvez configurer l'appliance pour qu'elle informe l'utilisateur des raisons pour lesquelles elle a bloqué la demande d'URL. Pour y parvenir, vous avez plusieurs possibilités :

Destinataire	Voir
Affichage des pages prédéfinies et personnalisables qui sont hébergées sur Secure Web Appliance.	Configuration des pages On-Box End-User Notification (Notification d'utilisateur final intégré), on page 377
Redirection de l'utilisateur vers les pages de notification HTTP à l'utilisateur final à une URL spécifique.	Pages Off-Box End-User Notification (Notification d'utilisateur final off-box) , on page 378

Configuration des pages On-Box End-User Notification (Notification d'utilisateur final intégré)

Before you begin

- Pour configurer la langue d'affichage et personnaliser le logo affiché, consultez Configuration des paramètres généraux pour les pages de notification, on page 372.
- Si vous souhaitez personnaliser le message affiché à l'aide des notifications intégrées, consultez les rubriques sous Messages personnalisés sur les pages de notification, on page 382. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 384.

Les pages intégrées sont des pages de notification prédéfinies et personnalisables qui se trouvent sur l'appliance.

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans le champ Notification Type (Type de notification), choisissez **Use On Box End User Notification** (Utiliser la notification de l'utilisateur final/intégrée).

Étape 4 Configurez les paramètres de la page de notification de l'utilisateur final/intégrée.

Paramètres	Description
Custom Message (Message personnalisé)	Incluez tout texte supplémentaire requis sur chaque page de notification. Lorsque vous saisissez un message personnalisé, AsyncOS place le message avant la dernière phrase sur la page de notification contenant les coordonnées.

Paramètres	Description
Contact Information (Coordonnées)	Personnaliser les coordonnées indiquées sur chaque page de notification. AsyncOS affiche la phrase de coordonnées comme dernière phrase d'une page, avant de fournir les codes de notification que les utilisateurs peuvent communiquer à l'administrateur réseau.
End-User Misclassification Reporting (Rapports sur les erreurs de classification de l'utilisateur final)	Si elle est activée, à partir d'AsyncOS 14.5, la demande de classification incorrecte est envoyée sur HTTPS. Vous ne recevrez aucune notification d'alerte de sécurité. Lorsque cette option est activée, les utilisateurs peuvent signaler à Cisco des URL mal classées. Un bouton supplémentaire s'affiche sur les pages On-Box End-User Notification (Notification d'utilisateur final intégré) pour les sites bloqués en raison d'une suspicion de logiciel ou de filtres d'URL malveillants. Ce bouton permet à l'utilisateur de signaler tout doute d'erreur de classification de la page. Il ne s'affiche pas pour les pages bloquées en raison d'autres paramètres de politique. **Note** • Vous devez activer la participation au réseau SenderBase. Consultez la section Activation de la participation au réseau Cisco SensorBase pour plus d'informations. • Vous devez avoir un compte Cisco valide associé au(x) numéro(s) de série de votre/vos appliances. • Le signalement des URL mal classées ne fonctionne pas sur les Secure Web Appliance virtuels.

Étape 5 (Facultatif) Cliquez sur le lien **Preview Notification Page Customization** (Survol de la personnalisation de la page de notification) pour afficher la page de notification de l'utilisateur final actuelle dans une fenêtre de navigateur distincte.

Note Si les fichiers HTML de notification ont été modifiés, cette fonctionnalité d'aperçu n'est pas disponible.

Étape 6 Envoyez et validez les modifications.

Pages Off-Box End-User Notification (Notification d'utilisateur final off-box)

Le proxy Web peut être configuré pour rediriger toutes les pages de notification HTTP à l'utilisateur final vers une URL spécifique que vous spécifiez.

Affichage de la page off-box correcte en fonction du motif du blocage de l'accès

Par défaut, AsyncOS redirige tous les sites Web bloqués vers l'URL, quelle que soit la raison pour laquelle il a bloqué la page d'origine. Cependant, AsyncOS transmet également des paramètres sous forme de chaîne de requête ajoutée à l'URL de redirection afin que vous puissiez vous assurer que l'utilisateur voit une page

unique expliquant la raison du blocage. Pour plus d'informations sur les paramètres inclus, consultez Paramètres de la page off-box des notifications envoyées à l'utilisateur final, on page 379.

Lorsque vous souhaitez que l'utilisateur affiche une page différente pour chaque raison d'un site Web bloqué, créez un script CGI sur le serveur Web qui peut analyser la chaîne de requête dans l'URL de redirection. Le serveur peut ensuite effectuer une deuxième redirection vers une page appropriée.

Critères d'URL pour les pages de notification off-box

- Vous pouvez utiliser n'importe quelle URL HTTP ou HTTPS.
- L'URL peut préciser un numéro de port précis.
- L'URL ne peut pas avoir d'arguments après le point d'interrogation.
- L'URL doit contenir un nom d'hôte bien formé.

Par exemple, si vous avez saisi l'URL suivante dans le champ Rediriger vers l'URL personnalisée :

```
http://www.example.com/eun.policy.html
```

Et vous avez l'entrée de journal des accès suivante :

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html HTTP/1.1
 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

Ensuite, AsyncOS crée l'URL redirigée suivante :

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

Paramètres de la page off-box des notifications envoyées à l'utilisateur final

AsyncOS transmet les paramètres au serveur Web en tant que paramètres d'URL standard dans la demande HTTP GET. Il utilise le format suivant :

```
<notification_page_url>?param1=value1&param2=value2
```

Le tableau décrit les paramètres qu'AsyncOS inclut dans la chaîne de requête.

Nom du paramètre	Description
Time (Durée)	Date et heure de la transaction.
ID (Identifiant)	ID de transaction.
Client_IP	Adresse IP du client.
User (Utilisateur)	Nom d'utilisateur du client ayant fait la demande, si celui-ci est disponible.
Site	Nom d'hôte de la destination dans la demande HTTP.
URI	Chemin d'accès URL spécifié dans la demande HTTP.

Nom du paramètre	Description
Status_Code	Code d'état HTTP de la demande.
Decision_Tag	Balise de décision ACL telle que définie dans l'entrée du journal d'accès qui indique comment le moteur DVS a géré la transaction.
URL_Cat	Catégorie d'URL attribuée par le moteur de filtrage d'URL à la demande de transaction. **Remarque :** AsyncOS pour le Web envoie le nom complet des catégories d'URL prédéfinies et définies par l'utilisateur. Il effectue l'encodage de l'URL sur le nom de la catégorie, de sorte que les espaces sont écrits comme « %20 ».
WBRS	Score WBRS que les filtres de réputation Web ont attribué à l'URL dans la demande.
DVS_Verdict	Catégorie de programme malveillant que le moteur DVS affecte à la transaction.
DVS_ThreatName	Nom du programme malveillant trouvé par le moteur DVS.
Reauth_URL	URL sur laquelle les utilisateurs peuvent cliquer pour s'authentifier à nouveau si l'utilisateur est bloqué sur un site Web en raison d'une politique de filtrage d'URL restrictive. Utilisez ce paramètre lorsque le paramètre d'authentification global « Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction » (Activer l'invite de réauthentification si l'utilisateur final est bloqué par la catégorie d'URL ou la restriction de session utilisateur) est activé et que l'utilisateur est bloqué sur un site Web en raison d'une catégorie d'URL bloquée. Pour utiliser ce paramètre, assurez-vous que le script CGI effectue les étapes suivantes : 1. Obtient la valeur du paramètre `Reauth_Url`. 2. Décode la valeur par URL-decode. 3. Décode la valeur par Base64 et obtient l'URL de réauthentification réelle. 4. Incluez l'URL décodée sur la page de notification de l'utilisateur final d'une manière ou d'une autre, sous la forme d'un lien ou d'un bouton, ainsi que des instructions à l'intention des utilisateurs pour les informer qu'ils peuvent cliquer sur le lien et saisir de nouveaux identifiants d'authentification qui permettent un accès amélioré.

Note AsyncOS inclut toujours tous les paramètres dans chaque URL redirigée. Si aucune valeur n'existe pour un paramètre particulier, AsyncOS transmet un tiret (-).

Redirection des pages End-User Notification (Notification d'utilisateur final) vers une URL personnalisée (off-box)

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la section **End-User Notification Pages** (Pages de notification d'utilisateur final), choisissez **Redirect to Custom URL** (Rediriger vers une URL personnalisée).

Étape 4 Dans le champ **Notification Page URL** (URL de la page de notification), saisissez l'URL vers laquelle vous souhaitez rediriger les sites Web bloqués.

Étape 5 (Facultatif) Cliquez sur **Preview Custom URL** (Survol du lien URL personnalisée).

Étape 6 Envoyez et validez les modifications.

Configuration de la page d'avertissement du filtrage des URL de l'utilisateur final

Before you begin

- Si vous souhaitez personnaliser le message affiché à l'aide des notifications intégrées, consultez les rubriques sous Messages personnalisés sur les pages de notification, on page 382. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 384.

Une page d'avertissement concernant le filtrage d'URL destinée à l'utilisateur final s'affiche lorsqu'un utilisateur accède pour la première fois à un site Web dans une catégorie d'URL particulière après un certain laps de temps. Vous pouvez également configurer la page d'avertissement lorsqu'un utilisateur accède au contenu pour adultes lorsque la fonction d'évaluation du contenu du site est activée.

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Faites défiler la liste jusqu'à la section d'avertissement concernant le filtrage des URL de l'utilisateur final.

Étape 4 Dans le champ Time Understanding (intervalle entre les avertissements), saisissez l'intervalle de temps utilisé par le proxy Web entre l'affichage de la page d'avertissement de filtrage des URL de l'utilisateur final pour chaque catégorie d'URL par utilisateur.

Vous pouvez indiquer n'importe quelle valeur comprise entre 30 et 2 678 400 secondes (un mois). La valeur par défaut est 1 heure (3 600 secondes). Vous pouvez entrer la valeur en secondes, minutes ou jours. Utilisez « s » pour les secondes, « m » pour les minutes et « d » pour les jours.

Étape 5 Dans le champ Message personnalisé, saisissez le texte que vous souhaitez voir apparaître sur chaque page d'avertissement de filtrage d'URL d'utilisateur final.

Étape 6 (Facultatif) Cliquez sur **Preview URL Category Warning Page Customization** (Survol de la personnalisation de la page d'avertissement de catégorie d'URL) pour afficher la page d'avertissement actuelle relative au filtrage des URL de l'utilisateur final dans une fenêtre de navigateur distincte.

Note Si les fichiers HTML de notification ont été modifiés, cette fonctionnalité d'aperçu n'est pas disponible.

Étape 7 Envoyez et validez les modifications.

Configuration des messages de notification FTP

Before you begin

Si vous souhaitez personnaliser le message affiché à l'aide des notifications intégrées, consultez les rubriques sous Messages personnalisés sur les pages de notification, on page 382. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 384.

Le proxy FTP affiche un message de notification prédéfini et personnalisable aux clients FTP natifs lorsqu'il ne peut pas établir de connexion avec le serveur FTP pour une raison, comme une erreur d'authentification par le proxy FTP ou une mauvaise réputation pour le nom de domaine du serveur. La notification est spécifique à la raison du blocage de la connexion.

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Faites défiler la liste jusqu'à la section FTP natif.

Étape 4 Dans le champ **Language** (Langue), sélectionnez la langue à utiliser lors de l'affichage des messages de notification FTP natifs.

Étape 5 Dans le champ **Custom Message** (Message personnalisé), saisissez le texte que vous souhaitez afficher dans chaque message de notification FTP natif.

Étape 6 Envoyez et validez les modifications.

Messages personnalisés sur les pages de notification

Les sections suivantes s'appliquent au texte saisi dans la zone « Custom Message » (Message personnalisé) pour tout type de notification configuré dans la page Edit End User Notification (Modifier la notification de l'utilisateur final).

- Balises HTML prises en charge dans les messages personnalisés sur les pages de notification, on page 382
- Mises en garde concernant les URL et les logos dans les pages de notification , on page 383

Balises HTML prises en charge dans les messages personnalisés sur les pages de notification

Vous pouvez utiliser des balises HTML pour mettre en forme le texte de n'importe quelle notification sur la page Modifier la notification de l'utilisateur final (Edit End User Notification) qui propose une zone « Custom Message » (Message personnalisé). Les balises doivent être en minuscules et respecter la syntaxe HTML standard (balises fermantes, etc.)

Vous pouvez utiliser les balises HTML suivantes.

- <a>
-

-
- <big></big>
-
- <code></code>
-
-
- <small></small>
-

Par exemple, vous pouvez mettre du texte en italique :

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

La balise vous permet d'utiliser n'importe quel style CSS pour mettre en forme le texte. Par exemple, vous pouvez afficher du texte en rouge :

```
 <span style="color: red">Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

Note Si vous avez besoin de plus de flexibilité ou si vous souhaitez ajouter du code JavaScript à vos pages de notification, vous devez modifier directement les fichiers de notification HTML. Le code JavaScript saisi dans la zone de message personnalisé pour les notifications dans l'interface utilisateur Web sera supprimé. Consultez Modification directe des fichiers HTML de la page de notification , on page 384.

Mises en garde concernant les URL et les logos dans les pages de notification

Cette section s'applique si vous effectuez l'une des personnalisations suivantes :

- Saisissez du texte dans la zone « Custom Message » (Message personnalisé) pour toute notification sur la page Edit End User Notification (Modifier la notification de l'utilisateur final).
- Modifier directement les fichiers HTML pour les notifications sur la boîte
- Utiliser un logo personnalisé

Toutes les combinaisons de chemins d'URL et de noms de domaine dans les liens intégrés dans un texte personnalisé et le logo personnalisé sont dispensés des éléments suivants pour les notifications sur la boîte :

- Authentification de l'utilisateur
- Accusé de réception de l'utilisateur final
- Toutes les analyses, comme l'analyse des programmes malveillants et l'évaluation de la réputation de sites Web

Par exemple, si les URL suivantes sont intégrées dans du texte personnalisé :

```
http://www.exemple.com/index.html
```

```
http://www.monentreprise.com/logo.jpg
```

Ensuite, toutes les URL suivantes seront également traitées comme dispensées de toute analyse :

```
http://www.exemple.com/index.html
```

```
http://www.monentreprise.com/logo.jpg
```

`http://www.exemple.com/logo.jpg`

`http://www.monentreprise.com/index.html`

Également, lorsqu'une URL intégrée est de la forme `<protocol>://<domain-name>/<directory path>/` Alors tous les sous-fichiers et sous-répertoires de ce chemin de répertoire sur l'hôte seront également exclus des tâches d'analyse.

Par exemple, si l'URL suivante est intégrée : `http://www.exemple.com/gallery2/`, les URL telles que `http://www.exemple.com/gallery2/main.PH` seront également traitées comme dispensées.

Cela vous permet de créer une page plus élaborée avec du contenu intégré tant que le contenu intégré est relatif à l'URL initiale. Cependant, vous devez également faire preuve de prudence lorsque vous décidez des chemins à inclure en tant que liens et logos personnalisés.

Modification directe des fichiers HTML de la page de notification

Chaque page de notification est stockée sur Secure Web Appliance au format HTML. Si vous avez besoin de plus de personnalisation que ne le permet la zone « Custom Message » (Message personnalisé) de l'interface Web, vous pouvez modifier directement ces fichiers HTML. Par exemple, vous pouvez inclure du code JavaScript standard ou modifier l'aspect général de chaque page.

Les renseignements dans les sections suivantes s'appliquent à tout type de fichier HTML de notification à l'utilisateur final sur l'appliance, y compris les pages d'accusé de réception de l'utilisateur final.

- Exigences relatives à la modification directe des fichiers HTML de notification , on page 384
- Modification directe des fichiers HTML de la page de notification , on page 384
- Utilisation de variables dans les fichiers HTML de notification , on page 385
- Variables de personnalisation des fichiers HTML de notification , on page 386

Exigences relatives à la modification directe des fichiers HTML de notification

- Chaque fichier d'échange de notification doit être un fichier HTML valide. Pour obtenir la liste des balises HTML que vous pouvez inclure, consultez Balises HTML prises en charge dans les messages personnalisés sur les pages de notification, on page 382.
- Les noms des fichiers d'échange de notifications doivent correspondre exactement aux noms des fichiers livrés avec Secure Web Appliance.

  Si le répertoire `configuration\eun` ne contient pas de fichier en particulier avec le nom requis, l'appliance affiche la page de notification standard de l'utilisateur final sur l'ordinateur.
- N'incluez aucun lien vers les URL dans les fichiers HTML. Tout lien inclus dans les pages de notification est soumis aux règles de contrôle d'accès définies dans les politiques d'accès et les utilisateurs peuvent se retrouver dans une boucle récursive.
- Testez vos fichiers HTML dans des navigateurs clients pris en charge pour vous assurer qu'ils se comportent comme prévu, en particulier s'ils comprennent du code JavaScript.

- Pour que vos pages personnalisées prennent effet, vous devez activer les fichiers personnalisés à l'aide de la commande d'interface de ligne de commande `advancedproxyconfig > EUN > Refresh EUN Pages`.

Modification directe des fichiers HTML de notification

Before you begin

- Prenez connaissance des exigences dans Exigences relatives à la modification directe des fichiers HTML de notification , on page 384.
- Consultez Variables de personnalisation des fichiers HTML de notification , on page 386 et Utilisation de variables dans les fichiers HTML de notification , on page 385.

Étape 1 Utilisez un client FTP pour vous connecter à Secure Web Appliance.

Étape 2 Accédez au répertoire `configuration\eun`.

Étape 3 Téléchargez les fichiers de répertoire de langue correspondant aux pages de notification que vous souhaitez modifier.

Étape 4 Sur votre ordinateur local, utilisez un éditeur de texte ou un éditeur HTML pour modifier les fichiers HTML.

Étape 5 Utilisez le client FTP pour charger les fichiers HTML personnalisés dans le répertoire à partir duquel vous les avez téléchargés à l'étape 3.

Étape 6 Ouvrez un client SSH et connectez-vous à Secure Web Appliance.

Étape 7 Exécutez la commande de l'interface de ligne de commande `advancedproxyconfig > EUN`.

Étape 8 Tapez **2** pour utiliser les pages de notification de l'utilisateur final personnalisées.

Étape 9 Si l'option de pages de notification de l'utilisateur final personnalisées est actuellement activée lorsque vous mettez à jour les fichiers HTML, saisissez **1** pour actualiser les pages de notification de l'utilisateur final personnalisées.

Si vous ne le faites pas, les nouveaux fichiers ne prendront effet qu'au redémarrage du proxy Web.

Étape 10 Validez vos modifications.

Étape 11 Fermez le client SSH.

Utilisation de variables dans les fichiers HTML de notification

Lorsque vous modifiez des fichiers HTML de notification, vous pouvez inclure des variables conditionnelles pour créer des instructions « if-then » pour effectuer différentes actions en fonction de l'état actuel.

Le tableau décrit les différents formats de variable conditionnelle.

Format de variable conditionnelle	Description
%?*V*	Cette variable conditionnelle évalue à TRUE si la sortie de la variable %*V* n'est pas vide.
%!*V*	Représente la condition suivante : `else` Utilisez cette condition avec la variable conditionnelle %?*V*.

Format de variable conditionnelle	Description
%#*V*	Représente la condition suivante : `endif` Utilisez cette condition avec la variable conditionnelle %?*V*.

Par exemple, le texte suivant est du code HTML qui utilise %R comme variable conditionnelle pour vérifier si la réauthentification est offerte, et %r comme variable normale pour fournir l'URL de réauthentification.

```
%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" OnClick="document.location='%r'" id="Reauth"
value="Login as different user...">
  </form>
</div>
%#R
```

Toute variable incluse dans Variables de personnalisation des fichiers HTML de notification , on page 386 peut être utilisée comme variable conditionnelle. Cependant, les meilleures variables à utiliser dans les instructions conditionnelles sont celles qui sont liées à la *demande du client* plutôt qu'à la réponse du serveur, et les variables qui peuvent ou non avoir la valeur TRUE au lieu des variables qui donnent toujours la valeur TRUE.

Variables de personnalisation des fichiers HTML de notification

Vous pouvez utiliser des variables dans les fichiers HTML de notification pour afficher des informations précises à l'utilisateur. Vous pouvez également convertir chaque variable en variable conditionnelle pour créer des instructions « if-then ». Pour en savoir plus, consultez Utilisation de variables dans les fichiers HTML de notification , on page 385.

Variable	Description	Toujours évaluée sur TRUE si elle est utilisée comme variable conditionnelle
%a	Domaine d'authentification pour FTP	Non
%A	Adresse ARP	Oui
%b	Nom de l'agent utilisateur	Non
%B	Motif du blocage, par exemple BLOCK-SRC ou BLOCK-TYPE	Non
%c	Personne-ressource dans la page d'erreur	Oui
%C	Ensemble complet - Témoin : ligne d'en-tête ou chaîne vide	Non
%d	Adresse IP du client	Oui
%D	Nom d'utilisateur	Non
%e	Adresse de messagerie de la page d'erreur	Oui

Variable	Description	Toujours évaluée sur TRUE si elle est utilisée comme variable conditionnelle
%E	URL du logo de la page d'erreur	Non
%f	Section de commentaires de l'utilisateur	Non
%F	URL pour les commentaires de l'utilisateur	Non
%g	Nom de la catégorie Web, si disponible	Oui
%G	Taille de fichier maximale (Mo)	Non
%h	Nom d'hôte du proxy	Oui
%H	Nom de serveur de l'URL	Oui
%i	Identifiant de transaction sous forme de nombre hexadécimal	Oui
%I	Management IP Address (adresse IP de gestion)	Oui
%j	Texte personnalisé de la page d'avertissement de catégorie d'URL	Non
%k	Lien de redirection vers la page d'accusé de réception de l'utilisateur final et la page d'avertissement du filtrage des URL de l'utilisateur final	Non
%K	Type de fichier de réponse	Non
%l	WWW-Authenticate : ligne d'en-tête	Non
%L	Proxy-Authenticate : ligne d'en-tête	Non
%M	La méthode de la demande, par exemple « GET » ou « POST »	Oui
%n	Nom de la catégorie de programmes malveillants, si disponible	Non
%N	Nom du programme malveillant, s'il est disponible	Non
%o	Type de menace pour la réputation Web, s'il est disponible	Non
%O	Motif de la menace pour la réputation Web, le cas échéant	Non
%p	Chaîne pour l'en-tête HTTP Proxy-Connection	Oui
%P	Protocole	Oui
%q	Nom du groupe de politiques d'identité	Oui
%Q	Nom du groupe de politiques pour les politiques autres que celles d'identité	Oui
%r	URL de redirection	Non

Variable	Description	Toujours évaluée sur TRUE si elle est utilisée comme variable conditionnelle
%R	Réauthentification proposée. Cette variable génère une chaîne vide lorsqu'elle est fausse et un espace lorsqu'elle est vraie, il n'est donc pas utile de l'utiliser seule. Utilisez-la plutôt comme variable de condition.	Non
%S	La signature du proxy	Non, toujours la valeur FALSE
%t	Horodatage en secondes Unix plus millisecondes	Oui
%T	La date	Oui
%u	La partie URI de l'URL (l'URL sans le nom du serveur)	Oui
%U	L'URL complète de la demande	Oui
%v	Version du protocole HTTP	Oui
%W	Port de gestion WebUI	Oui
%X	Code de blocage étendu Il s'agit d'une valeur base64 de 16 octets qui code la plupart des informations de réputation Web et de protection contre les programmes malveillants enregistrées dans le journal des accès, telles que la balise de décision ACL et le score WBRS.	Oui
%Y	Chaîne de texte personnalisée de l'administrateur, si définie, vide sinon	Non
%y	Texte personnalisé de la page d'accusé de réception de l'utilisateur final	Oui
%z	Niveau de réputation Web	Oui
%Z	Métadonnées DLP	Oui
%%	Imprime le symbole de pourcentage (%) dans la page de notification	s.o.

Types de pages de notification

Par défaut, le proxy Web affiche une page de notification indiquant aux utilisateurs qu'ils ont été bloqués et la raison du blocage.

La plupart des pages de notification affichent un ensemble de codes différent qui peut aider les administrateurs ou l'assistance client de Cisco à résoudre tout problème potentiel. Certains codes sont réservés à un usage interne chez Cisco. Les différents codes qui peuvent s'afficher dans les pages de notification sont identiques aux variables que vous pouvez inclure dans les pages de notification personnalisées, comme indiqué dans Variables de personnalisation des fichiers HTML de notification , on page 386.

Le tableau décrit les différentes pages de notification que les utilisateurs peuvent rencontrer.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_ACCEPTED Commentaires acceptés, merci	Page de notification qui s'affiche après que les utilisateurs ont utilisé l'option « Report Misclassification » (Signaler une erreur de classification).	Le rapport de classification incorrecte a été envoyé. Nous vous remercions de vos commentaires.
ERR_ADAPTIVE_SECURITY Politique : générale	Bloque la page qui s'affiche lorsque l'utilisateur est bloqué en raison de la fonctionnalité d'analyse adaptative.	En fonction des politiques de sécurité de votre entreprise, le site Web <*URL* > a été bloqué, car son contenu a été considéré comme un risque pour la sécurité.
ERR_ADULT_CONTENT Politique : accusé de réception	Page d'avertissement qui s'affiche lorsque l'utilisateur final accède à une page classée comme contenu pour adultes. Les utilisateurs peuvent cliquer sur un lien d'accusé de réception pour continuer vers le site initialement demandé.	Vous essayez de visiter une page Web dont le contenu est classé comme explicite ou réservé aux adultes. En cliquant sur le lien ci-dessous, vous reconnaissez avoir lu et accepté les politiques de l'organisation qui régissent l'utilisation d'Internet pour ce type de contenu. Les données concernant votre comportement de navigation peuvent être surveillées et enregistrées. Il vous sera régulièrement demandé de confirmer cette déclaration pour continuer à accéder à ce type de page Web. Cliquez ici pour accepter cette déclaration et accéder à Internet.
ERR_AVC Politique : contrôles des applications	Page de blocage qui s'affiche lorsque l'utilisateur est bloqué en raison du moteur de visibilité et de contrôle des applications.	Selon les politiques d'accès de votre organisation, l'accès à l'application %1 de type %2 a été bloqué.
ERR_BAD_REQUEST Demande incorrecte	Page d'erreur résultant d'une demande de transaction non valide.	Le système ne peut pas traiter cette demande. Un navigateur non standard a peut-être généré une requête HTTP non valide. Si vous utilisez un navigateur standard, réessayez la demande.
ERR_BLOCK_DEST Politique : destination	Page de blocage qui s'affiche lorsque l'utilisateur tente d'accéder à une adresse de site Web bloquée.	Selon les politiques d'accès de votre organisation, l'accès au site Web <*URL* > a été bloqué.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_BROWSER Sécurité : navigateur	Page de blocage qui s'affiche lorsque la demande de transaction émane d'une application qui a été identifiée comme menacée par un programme malveillant ou un logiciel espion.	Selon les politiques d'accès de votre organisation, les demandes de votre ordinateur ont été bloquées, car il a été déterminé qu'il s'agit d'une menace pour le réseau de l'organisation. Votre navigateur a peut-être été compromis par un programme malveillant ou un logiciel espion identifié comme « [*nom du programme malveillant*] ». Veuillez communiquer avec <*contact name* > <*email address* > et indiquez les codes présentés ci-dessous. Si vous utilisez un navigateur non standard et pensez qu'il a été mal classé, utilisez le bouton ci-dessous pour signaler cette erreur de classification.
ERR_BROWSER_CUSTOM Politique : navigateur	Page de blocage qui s'affiche lorsque la demande de transaction provient d'un agent utilisateur bloqué.	Selon les politiques d'accès de votre organisation, les demandes de votre navigateur ont été bloquées. Ce navigateur « <*browser type* > » n'est pas autorisé en raison de risques pour la sécurité potentiels.
ERR_CERT_INVALID Certificat non valide	Page de blocage qui s'affiche lorsque le site HTTPS demandé utilise un certificat non valide.	Une session sécurisée n'a pas pu être établie, car le site <*hostname* > a fourni un certificat non valide.
ERR_CONTINUE_ UNACKNOWLEDGED Politique : accusé de réception	Page d'avertissement qui s'affiche lorsque l'utilisateur demande un site qui fait partie d'une catégorie d'URL personnalisée à laquelle l'action avertir est affectée. Les utilisateurs peuvent cliquer sur un lien d'accusé de réception pour continuer vers le site initialement demandé.	Vous essayez de consulter une page Web qui appartient à la catégorie d'URL <*URL category* >. En cliquant sur le lien ci-dessous, vous reconnaissez avoir lu et accepté les politiques de l'organisation qui régissent l'utilisation d'Internet pour ce type de contenu. Les données concernant votre comportement de navigation peuvent être surveillées et enregistrées. Il vous sera régulièrement demandé de confirmer cette déclaration pour continuer à accéder à ce type de page Web. Cliquez ici pour accepter cette déclaration et accéder à Internet.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_DNS_FAIL Échec du DNS	Page d'erreur qui s'affiche lorsque l'URL demandée contient un nom de domaine non valide.	La résolution du nom d'hôte (recherche DNS) pour ce nom d'hôte <*hostname* > a échoué. L'adresse Internet est peut-être mal épelée ou obsolète, l'hôte <*hostname* > peut être temporairement indisponible ou le serveur DNS peut ne pas répondre. Veuillez vérifier l'orthographe de l'adresse Internet saisie. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_EXPECTATION_ FAILED Échec de l'attente	Page d'erreur qui s'affiche lorsque la demande de transaction déclenche la réponse HTTP 417 « Expectation Failed » (Échec de l'attente).	Le système ne peut pas traiter la demande pour ce site| Un navigateur non standard a peut-être généré une requête HTTP non valide. Si vous utilisez un navigateur standard, réessayez la demande.
ERR_FILE_SIZE Politique : taille du fichier	Page de blocage qui s'affiche lorsque le fichier demandé est plus volumineux que la taille de fichier maximale autorisée.	Selon les politiques d'accès de votre organisation, l'accès à ce site Web ou <*URL* > de téléchargement a été bloqué, car la taille du téléchargement dépasse la limite autorisée.
ERR_FILE_TYPE Politique : type de fichier	Page de blocage qui s'affiche lorsque le fichier demandé est de type bloqué.	Selon les politiques d'accès de votre organisation, l'accès à ce site Web ou <*URL* > de téléchargement a été bloqué, car le type de fichier « <*file type* > » n'est pas autorisé.
ERR_FILTER_FAILURE Échec du filtre	Page d'erreur qui s'affiche lorsque le moteur de filtrage d'URL est temporairement incapable de fournir une réponse de filtrage d'URL et que l'option « action par défaut pour le service inaccessible » est définie sur Block (Bloquer).	La demande de la page <*URL* > a été refusée, car un serveur interne est actuellement inaccessible ou surchargé. Veuillez réessayer la demande plus tard.
ERR_FOUND Trouvé	Page de redirection interne pour certaines erreurs.	La page <*URL* > est redirigée vers <*redirected URL* >.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_FTP_ABORTED FTP abandonné	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP déclenche la réponse HTTP 416 « Requested Plage Not Satisfiable » (Plage demandée impossible à satisfaire).	La demande pour le fichier <*URL* > n'a pas réussi. Le serveur FTP <*hostname* > a mis fin à la connexion de manière inattendue. Veuillez réessayer la demande plus tard.
ERR_FTP_AUTH_ REQUIRED Autorisation FTP requise	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP déclenche la réponse FTP 530 « Not Logded In » (Pas connecté).	L'authentification est requise par le serveur FTP <*hostname* >. Un identifiant d'utilisateur et une phrase secrète valides doivent être saisis lorsque vous y êtes invité. Dans certains cas, le serveur FTP peut limiter le nombre de connexions anonymes. Si vous vous connectez habituellement à ce serveur en tant qu'utilisateur anonyme, veuillez réessayer plus tard.
ERR_FTP_CONNECTION_ FAILED Échec de connexion FTP	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP déclenche la réponse FTP 425 « Can't open data connection » (Impossible d'ouvrir la connexion de données).	Le système ne peut pas communiquer avec le serveur FTP <*hostname* >. Le serveur FTP est peut-être hors service de façon temporaire ou permanente, ou peut être inaccessible en raison de problèmes de réseau. Veuillez vérifier l'orthographe de l'adresse saisie. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_FTP_FORBIDDEN FTP interdit	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP concerne un objet auquel l'utilisateur n'est pas autorisé à accéder.	L'accès a été refusé par le serveur FTP <*hostname* >. Votre ID utilisateur n'a pas l'autorisation d'accéder à ce document.
ERR_FTP_NOT_FOUND FTP introuvable	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP concerne un objet qui n'existe pas sur le serveur.	Le fichier <*URL* > est introuvable. L'adresse est incorrecte ou obsolète.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_FTP_SERVER_ERR Erreur du serveur FTP	Page d'erreur qui s'affiche pour les transactions FTP sur HTTP qui tentent d'accéder à un serveur qui ne prend pas en charge FTP. Le serveur renvoie généralement la réponse HTTP 501 « Not Implemented » (Non mis en œuvre).	Le système ne peut pas communiquer avec le serveur FTP <*hostname* >. Le serveur FTP peut être en panne de façon temporaire ou permanente, ou peut ne pas fournir ce service. Veuillez confirmer qu'il s'agit d'une adresse valide. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_FTP_SERVICE_ UNAVAIL Service FTP non disponible	Page d'erreur qui s'affiche pour les transactions FTP sur HTTP qui tentent d'accéder à un serveur FTP qui n'est pas disponible.	Le système ne peut pas communiquer avec le serveur FTP <*hostname* >. Le serveur FTP est peut-être occupé, en panne permanente ou ne fournit pas ce service. Veuillez confirmer qu'il s'agit d'une adresse valide. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_GATEWAY_TIMEOUT Expiration de la passerelle	Page d'erreur qui s'affiche lorsque le serveur demandé n'a pas reçu de réponse en temps opportun.	Le système ne peut pas communiquer avec le serveur externe <*hostname* >. Le serveur Internet est peut-être occupé, en panne permanente ou inaccessible en raison de problèmes de réseau. Veuillez vérifier l'orthographe de l'adresse Internet saisie. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_IDS_ACCESS_ FORBIDDEN Accès IDS interdit	Page de blocage qui s'affiche lorsque l'utilisateur tente de charger un fichier bloqué en raison d'une politique de sécurité des données Cisco configurée.	Votre demande de téléchargement a été bloquée en fonction des politiques de transfert de données de votre organisation. Détails des fichiers : <*file details* >
ERR_INTERNAL_ERROR Erreur interne	Page d'erreur qui s'affiche en cas d'erreur interne.	Erreur de système interne lors du traitement de la demande pour la page <*URL* >. Veuillez réessayer cette demande. Si ce problème persiste, veuillez communiquer avec <*contact name* > <*email address* > et lui communiquer le code indiqué ci-dessous.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_MALWARE_ SPECIFIC Sécurité : programme malveillant détecté	Page de blocage qui s'affiche lorsqu'un programme malveillant est détecté lors du téléchargement d'un fichier.	Selon les politiques d'accès de votre entreprise, ce site Web <*URL* > a été bloqué, car il a été considéré comme une menace pour votre ordinateur ou le réseau de l'entreprise. Un programme malveillant <*nom* du programme malveillant> dans la catégorie <*catégorie du programme malveillant* > a été détecté sur ce site.
ERR_MALWARE_ SPECIFIC_OUTGOING Sécurité : programme malveillant détecté	Page de blocage qui s'affiche lorsqu'un programme malveillant est détecté lors du chargement d'un fichier.	Conformément à la politique de votre organisation, le téléchargement du fichier vers l'URL (<*URL* >) a été bloqué, car il a été détecté que le fichier contenait des logiciels malveillants susceptibles de nuire à la sécurité du réseau du destinataire. Nom du programme malveillant : <*malware name* > Catégorie du programme malveillant : <*malware category* >
ERR_NATIVE_FTP_DENIED	Message de blocage affiché dans les clients FTP natifs lorsque la transaction FTP native est bloquée.	530 Connexion refusée
ERR_NO_MORE_ FORWARDS Plus de transferts	Page d'erreur qui s'affiche lorsque l'appliance a détecté une boucle vers l'avant entre le proxy Web et un autre serveur proxy du réseau. Le proxy Web interrompt la boucle et affiche ce message pour le client.	La demande pour la page <*URL* > a échoué. Il se peut que l'adresse du serveur <*hostname* > ne soit pas valide ou vous devrez peut-être préciser un numéro de port pour accéder à ce serveur.
ERR_POLICY Politique : générale	Page de blocage qui s'affiche lorsque la demande est bloquée par un paramètre de politique.	Selon les politiques d'accès de votre organisation, l'accès au site Web <*URL* > a été bloqué.
ERR_PROTOCOL Politique : protocole	Page de blocage qui s'affiche lorsque la demande est bloquée en fonction du protocole utilisé.	Selon les politiques d'accès de votre organisation, cette demande a été bloquée, car le protocole de transfert de données « <*protocol type* > » n'est pas autorisé.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_PROXY_AUTH_REQUIRED Autorisation du proxy requise.	Page de notification qui s'affiche lorsque les utilisateurs doivent saisir leurs informations d'authentification pour continuer. Ceci est utilisé pour les demandes de transaction explicites.	Une authentification est requise pour accéder à Internet à l'aide de ce système. Un identifiant d'utilisateur et une phrase secrète valides doivent être saisis lorsque vous y êtes invité.
ERR_PROXY_PREVENT_MULTIPLE_LOGIN Déjà connecté à partir d'un autre appareil	Page de blocage qui s'affiche quand un utilisateur tente d'accéder au Web en utilisant le même nom d'utilisateur que celui qui est déjà authentifié auprès du proxy Web sur un autre appareil. Cette fonctionnalité est utilisée lorsque l'option d'authentification globale User Session Restrictions (Restrictions des sessions utilisateur) est activée.	Selon les politiques de votre organisation, la demande d'accès à Internet a été refusée, car cet identifiant d'utilisateur dispose d'une session active à partir d'une autre adresse IP. Si vous souhaitez vous connecter sous un nom d'utilisateur différent, cliquez sur le bouton ci-dessous et entrez un nom d'utilisateur et une phrase secrète différents.
ERR_PROXY_REDIRECT Rediriger	Page de redirection.	Cette demande est en cours de redirection. Si cette page n'est pas automatiquement redirigée, cliquez ici pour continuer.
ERR_PROXY_UNACKNOWLEDGED Politique : accusé de réception	Page de confirmation de l'utilisateur final. Pour en savoir plus, consultez Pages End-User Notification (Notification d'utilisateur final) , on page 377.	Veuillez accepter les déclarations suivantes avant d'accéder à Internet. Vos transactions Web seront automatiquement surveillées et traitées pour détecter le contenu dangereux et appliquer les politiques de l'entreprise. En cliquant sur le lien ci-dessous, vous reconnaissez cette supervision et acceptez que des données concernant les sites que vous visitez puissent être enregistrées. Il vous sera régulièrement demandé d'accepter la présence du système de supervision. Vous êtes responsable du respect des politiques de l'entreprise en matière d'accès à Internet. Cliquez ici pour accepter cette déclaration et accéder à Internet.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_PROXY_ UNLICENSED Proxy sans licence	Page de blocage qui s'affiche lorsqu'il n'y a pas de clé de licence valide pour le proxy Web Secure Web Appliance.	L'accès à Internet n'est pas disponible sans une licence appropriée du périphérique de sécurité. Veuillez communiquer avec <*contact name* > <*email address* > et lui indiquer le code présenté ci-dessous. **Note** Pour accéder à l'interface de gestion du périphérique de sécurité, entrez l'adresse IP configurée avec port.
ERR_RANGE_NOT_ SATISFIABLE Plage impossible à satisfaire	Page d'erreur qui s'affiche lorsque la plage d'octets demandée ne peut pas être traitée par le serveur Web.	Le système ne peut pas traiter cette demande. Un navigateur non standard a peut-être généré une requête HTTP non valide. Si vous utilisez un navigateur standard, réessayez la demande.
ERR_REDIRECT_ PERMANENT Redirection permanente	Page de redirection interne.	La page <*URL* > est redirigée vers <*redirected URL* >.
ERR_REDIRECT_REPEAT_ REQUEST Rediriger	Page de redirection interne.	Veuillez renouveler votre demande.
ERR_SAAS_AUTHENTICATION Politique : accès refusé	Page de notification qui s'affiche lorsque les utilisateurs doivent saisir leurs informations d'authentification pour continuer. Ceci est utilisé pour accéder aux applications.	Selon la politique de votre organisation, la demande d'accès à <*URL*> a été redirigée vers une page où vous devez saisir les coordonnées de connexion. Vous serez autorisé à accéder à l'application si l'authentification réussit et si vous disposez des privilèges appropriés.
ERR_SAAS_AUTHORIZATION Politique : accès refusé	Page de blocage qui s'affiche lorsque les utilisateurs tentent d'accéder à une application à laquelle ils n'ont pas accès.	Selon la politique de votre organisation, l'accès à l'application <*URL* > est bloqué, car vous n'êtes pas un utilisateur autorisé. Si vous souhaitez vous connecter sous un autre nom d'utilisateur, entrez un nom d'utilisateur et une phrase secrète différents pour l'utilisateur autorisé à accéder à cette application.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_SAML_PROCESSING Politique : accès refusé	Page d'erreur qui s'affiche lorsqu'un processus interne échoue en tentant de traiter l'URL de connexion unique pour accéder à une application.	La demande d'accès de <*nom d'utilisateur* > n'a pas été retenue, car des erreurs ont été trouvées au cours du processus de la demande de connexion unique.
ERR_SERVER_NAME_EXPANSION Extension du nom du serveur	Page de redirection interne qui développe automatiquement l'URL et redirige les utilisateurs vers l'URL mise à jour.	Le nom du serveur <*hostname* > semble être une abréviation et est redirigé vers <*redirected URL* >.
ERR_URI_TOO_LONG URI trop long	Page de blocage qui s'affiche lorsque la longueur de l'URL est trop longue.	L'URL demandée était trop longue et n'a pas pu être traitée. Il peut s'agir d'une attaque contre votre réseau. Veuillez communiquer avec <*contact name* > <*email address* > et lui indiquer le code présenté ci-dessous.
ERR_WBRS Sécurité : risque lié aux programmes malveillants	Page de blocage qui s'affiche lorsque les filtres de réputation Web bloquent le site en raison d'un faible score de réputation Web.	Selon les politiques d'accès de votre entreprise, ce site Web <*URL* > a été bloqué, car les filtres de réputation Web ont déterminé qu'il constitue une menace pour votre ordinateur ou le réseau de l'entreprise. Ce site Web a été associé à des programmes malveillants et espions. Type de menace : %o Motif de la menace : %O
ERR_WEBCAT Politique : filtrage d'URL	Page de blocage qui s'affiche lorsque les utilisateurs tentent d'accéder à un site Web dans une catégorie d'URL bloquée.	Selon les politiques d'accès de votre organisation, l'accès à ce site Web <*URL* > a été bloqué, car la catégorie Web « <*category type* > » n'est pas autorisée.
ERR_WWW_AUTH_REQUIRED Autorisation WWW requise.	Page de notification qui s'affiche lorsque le serveur demandé demande aux utilisateurs de saisir leurs informations d'authentification pour continuer.	Une authentification est requise pour accéder au site Web <*hostname* > demandé. Un identifiant d'utilisateur et une phrase secrète valides doivent être saisis lorsque vous y êtes invité.

CHAPITRE 18

Générer des rapports pour superviser l'activité de l'utilisateur final

Cette rubrique contient les sections suivantes :

Survol de la génération de rapports

Secure Web Appliance génère des rapports généraux qui vous permettent de comprendre ce qui se passe sur le réseau et d'afficher les détails du trafic pour un domaine, un utilisateur ou une catégorie en particulier. Vous pouvez exécuter des rapports pour afficher un affichage interactif de l'activité du système sur une période donnée, ou vous pouvez planifier des rapports et les exécuter à des intervalles réguliers.

Thèmes connexes

- Impression et exportation des rapports à partir des pages de rapport, on page 405

Utilisation des noms d'utilisateur dans les rapports

Lorsque vous activez l'authentification, les rapports répertorient les utilisateurs en fonction de leur nom d'utilisateur lorsqu'ils s'authentifient avec le proxy Web. Par défaut, les noms d'utilisateurs sont écrits tels qu'ils apparaissent sur le serveur d'authentification. Cependant, vous pouvez choisir de rendre les noms d'utilisateurs non reconnaissables dans tous les rapports.

Note Les administrateurs peuvent toujours voir les noms d'utilisateurs dans les rapports.

Étape 1 Choisissez **Security Services > Reporting** (Services de sécurité > Rapports), puis cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 2 Sous Local Reporting (Rapports locaux), sélectionnez **Anonymize usernames in reports** (Anonymiser les noms d'utilisateur dans les rapports).

Étape 3 Envoyez et validez les modifications.

Pages de rapport

Secure Web Appliance propose les rapports suivants :

- My Dashboard (Mon tableau de bord) (« page d'accueil » de la création de rapports; ce rapport est également accessible en cliquant sur l'icône d'accueil dans le bord gauche de la barre de menus)
- Survol
- Users (Utilisateurs)
- Nombre d'utilisateurs
- Sites Web
- URL Categories (Catégories d'URL)
- Visibilité de l'application
- Protection contre les programmes malveillants
- Cisco Secure Endpoint
- Analyse de fichier
- Mises à jour des verdicts Cisco Secure Endpoint
- Risques de programmes malveillants des clients
- Web Reputation Filters (Filtres de réputation Web)
- L4 Traffic Monitor (Supervision du trafic de la couche 4)
- Proxy SOCKS
- Rapports par emplacement d'utilisateur
- Suivi Web
- Capacité du système
- État du système
- Rapports planifiés
- Rapports archivés

Utilisation des pages de rapports

Les différentes pages de rapport fournissent un aperçu de l'activité du système et prennent en charge plusieurs options pour l'affichage des données du système. Vous pouvez également rechercher dans chaque page un site Web et des données propres aux clients.

Vous pouvez effectuer les tâches suivantes sur la plupart des pages de rapport :

Option	Lien vers la tâche
Modifier la plage de temps affichée dans un rapport	Modification de la plage de temps, on page 401
Rechercher des clients et des domaines spécifiques	Recherche de données, on page 402
Choisir les données à afficher dans les graphiques	Choix des données à représenter au format graphique , on page 403
Exporter des rapports vers des fichiers externes	Impression et exportation des rapports à partir des pages de rapport, on page 405

Modification de la plage de temps

Vous pouvez mettre à jour les données affichées pour chaque composant de sécurité en utilisant le champ Time Range (Plage de temps). Cette option vous permet de générer des mises à jour pour des plages de temps prédéfinies et de définir des plages de temps personnalisées d'une heure de début précise à une heure de fin précise.

Note La plage de temps que vous sélectionnez est utilisée dans toutes les pages du rapport jusqu'à ce que vous sélectionniez une valeur différente dans le menu Time Range (Plage de temps).

Time Range (Plage de temps)	Les données sont retournées en...
Hour (Heure)	Soixante minutes complètes, plus jusqu'à cinq minutes supplémentaires.
Day (Jour)	Intervalles d'une heure pour les dernières 24 heures et incluant l'heure partielle actuelle.
Week (Semaine)	Intervalles d'une journée pour les 7 derniers jours plus le jour partiel courant.
Mois (30 jours)	Intervalles d'un journée pour les 30 derniers jours plus le jour partiel courant.
Hier	Les dernières 24 heures (00:00 à 23:59) en utilisant le fuseau horaire défini dans Secure Web Appliance.

Time Range (Plage de temps)	Les données sont retournées en...
Plage personnalisée	La plage de temps personnalisée que vous avez définie. Lorsque vous choisissez Custom Range (Plage personnalisée), une boîte de dialogue s'affiche pour vous permettre de saisir les heures de début et de fin.

Note Tous les rapports affichent des informations de date et d'heure en fonction du fuseau horaire configuré pour le système, indiqué par un décalage par rapport à l'heure de Greenwich (GMT). Cependant, les exportations de données affichent l'heure GMT uniquement pour s'adapter à plusieurs systèmes couvrant plusieurs fuseaux horaires à travers le monde.

Choix d'une plage de temps pour les rapports

La plupart des pages de rapports prédéfinies vous permettent de choisir une plage de temps pour les données à inclure. La plage de temps que vous sélectionnez est utilisée pour toutes les pages du rapport jusqu'à ce que vous sélectionniez une valeur différente dans le menu Time Range (Plage de temps).

Les options de plage de temps disponibles varient en fonction de l'appliance et selon les rapports par courriel et sur le Web sur l'appliance de gestion de la sécurité :

Note Les plages de temps sur les pages de rapport sont affichées en tant que décalage par rapport à l'heure de Greenwich (GMT). Par exemple, l'heure du Pacifique est GMT + 7 heures (GMT + 07:00).

Note Tous les rapports affichent des informations de date et d'heure en fonction du fuseau horaire configuré dans les systèmes, indiqué par un décalage par rapport à l'heure de Greenwich (GMT). Cependant, les exportations de données affichent l'heure GMT pour s'adapter à plusieurs systèmes dans plusieurs fuseaux horaires à travers le monde.

Recherche de données

Certains rapports comprennent un champ que vous pouvez utiliser pour rechercher des points de données particuliers. Lorsque vous recherchez des données, le rapport affine les données du rapport pour l'ensemble de données particulier que vous recherchez. Vous pouvez rechercher les valeurs qui correspondent exactement à la chaîne que vous entrez ou qui commencent par la chaîne que vous entrez. Les pages de rapport suivantes comprennent des champs de recherche :

Champs de recherche	Description
Users (Utilisateurs)	Recherchez un utilisateur par nom d'utilisateur ou adresse IP du client.

Champs de recherche	Description
Web Sites (Sites Web)	Recherchez un serveur par domaine ou adresse IP de serveur.
URL Categories (Catégories d'URL)	Recherchez une catégorie d'URL.
Application Visibility (Visibilité de l'application)	Recherchez un nom d'application que le moteur AVC surveille et bloque.
Client Malware Risk (Risque lié aux programmes malveillants pour le client)	Recherchez un utilisateur par nom d'utilisateur ou adresse IP du client.

Note Vous devez configurer l'authentification pour afficher les ID des utilisateurs clients ainsi que les adresses IP des clients.

Choix des données à représenter au format graphique

Les tableaux par défaut dans chaque page de rapports Web affichent les données couramment référencées, mais vous pouvez choisir d'afficher des données différentes à la place. Si une page contient plusieurs graphiques, vous pouvez modifier chaque graphique. Les options de tableau sont les mêmes que les en-têtes de colonne du ou des tableaux du rapport.

Étape 1 Cliquez sur le lien **Chart Options** (Options du graphique) sous un graphique.

Étape 2 Choisissez les données à afficher.

Étape 3 Cliquez sur **Done** (Terminé).

Rapports personnalisés

Vous pouvez créer une page de rapport personnalisée sur la en assemblant des graphiques et des tableaux à partir de pages de rapport existantes.

Destinataire	Faire ceci
Ajouter des modules à votre page de rapport personnalisé	Voir : • Modules ne pouvant pas être ajoutés aux rapports personnalisés , on page 404. • Création de votre page de rapports personnalisés , on page 404
Afficher votre page de rapport personnalisé	1. Choisissez **Monitor > Email or Web > Reporting > Reporting > My Reports** (Superviser > E-mail ou Web > Rapports > Rapports > Mes rapports). 2. Sélectionnez la plage de temps pour afficherla plage de temps sélectionnée s'applique à tous les rapports, notamment tous les modules de la page My Reports (Mes rapports). Les nouveaux modules ajoutés s'affichent en haut du rapport personnalisé.

Destinataire	Faire ceci
Réorganiser les modules sur votre page de rapport personnalisé	Faites glisser et déposez les modules à l'emplacement souhaité.
Supprimer des modules de votre page de rapport personnalisé	Cliquez sur le [X] dans le coin supérieur droit du module.
Générer une version PDF ou CSV de votre rapport personnalisé	Choisissez **Reporting > Archived Reports** (Rapports > Rapports archivés) et cliquez sur **Generate Report Now** (Générer un rapport maintenant).
Générer régulièrement une version PDF ou CSV de votre rapport personnalisé	Choisissez **Reporting > Scheduled Reports** (Rapports > Rapports planifiés).

Modules ne pouvant pas être ajoutés aux rapports personnalisés

- Résultats de la recherche , y compris les résultats de la recherche de suivi Web

Création de votre page de rapports personnalisés

Before you begin

- Assurez-vous que les modules que vous souhaitez ajouter peuvent l'être. Consultez Modules ne pouvant pas être ajoutés aux rapports personnalisés , on page 404.
- Supprimez tous les modules par défaut dont vous n'avez pas besoin en cliquant sur le [**X**] dans le coin supérieur droit de ces modules.

Étape 1 Utilisez l'une des méthodes suivantes pour ajouter un module à votre page de rapport personnalisée :

Note Certains modules ne sont disponibles que si vous utilisez une de ces méthodes. Si vous ne pouvez pas ajouter de module en utilisant une méthode, essayez une autre méthode.

- Accédez à la page du rapport sous l'onglet contenant le module que vous souhaitez ajouter, puis cliquez sur le bouton [+] en haut du module.
- Accédez à **Reporting** > **My Reports** (Web > Rapports > Mes Rapports), cliquez sur le bouton [+] (Module de rapport) en haut de l'une des sections, puis sélectionnez le module de rapport que vous voulez ajouter. Vous devrez peut-être cliquer sur [+] (Module du rapport) afin de rechercher le module qui vous intéresse.

  Vous ne pouvez ajouter chaque module qu'une seule fois; si vous avez déjà ajouté un module en particulier à votre rapport, l'option permettant de l'ajouter ne sera pas disponible.

Étape 2 Si vous ajoutez un module que vous avez personnalisé (p. ex., en ajoutant, en supprimant ou en réordonnant des colonnes, ou en affichant des données autres que celles par défaut dans le tableau), personnalisez les modules sur la page My Reports (Mes rapports).

Les modules sont ajoutés avec les paramètres par défaut. La plage de temps du module d'origine n'est pas conservée.

Étape 3 Si vous ajoutez un graphique qui inclut une légende distincte (par exemple, un graphique de la page de survol), ajoutez la légende séparément. Si nécessaire, faites-la glisser et déposez-la à côté des données qu'elle décrit.

Sous-domaines comparés aux domaines de deuxième niveau dans les rapports et le suivi

Dans le cadre des recherches de rapport et de suivi, les domaines de deuxième niveau (les domaines régionaux figurent à l'adresse http://george.surbl.org/two-level-tlds) sont traités différemment des sous-domaines, bien que les deux types de domaines puissent sembler être identiques. Par exemple :

- Les rapports n'incluront pas les résultats pour un domaine à deux niveaux comme `co.uk`, mais incluront les résultats pour `foo.co.uk`. Les rapports incluent les sous-domaines du domaine principal de l'entreprise, par exemple, `cisco.com`.
- Le suivi des résultats de recherche pour le domaine régional `co.uk` n'inclura pas les domaines comme `foo.co.uk`, tandis que les résultats de recherche pour `cisco.com` incluront les sous-domaines comme `sous-domaine.cisco.com`.

Impression et exportation des rapports à partir des pages de rapport

Vous pouvez générer une version PDF au format PDF de n'importe quelle page de rapport en cliquant sur le lien **Printable (PDF)** (Imprimable (PDF)) dans le coin supérieur droit de la page. Vous pouvez également exporter des données brutes sous forme de fichier de valeurs séparées par des virgules (CSV) en cliquant sur le lien **Export** (Exporter).

Étant donné que les exportations CSV n'incluent que des données brutes, les données exportées à partir d'une page de rapport Web peuvent ne pas inclure de données calculées telles que des pourcentages, même si ces données apparaissent dans le rapport Web.

Exportation des données du rapport

La plupart des rapports comprennent un lien d'**exportation** qui vous permet d'exporter des données brutes vers un fichier de valeurs séparées par des virgules (CSV). Après avoir exporté les données vers un fichier CSV, vous pouvez accéder aux données qu'il contient et les manipuler à l'aide d'applications telles que Microsoft Excel.

Les données CSV exportées affichent toutes les données de suivi des messages et de rapports selon le temps moyen de Greenwich (GMT), quel que soit le fuseau horaire défini sur Secure Web Appliance. Le but de la conversion de l'heure GMT est de permettre aux données d'être utilisées indépendamment de l'appliance ou lors du référencement de données à partir d'appliances se trouvent dans plusieurs fuseaux horaires.

L'exemple suivant est une entrée issue d'une exportation de données brutes du rapport sur la catégorie de protection contre les programmes malveillants, où l'heure avancée du Pacifique (PDT) est remplacée par GMT 07:00 :

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
 Transactions Monitored, Transactions Blocked, Transactions Detected
```

```
 1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100,
2625
```

En-tête de catégorie	Valeur	Description
`Begin Timestamp` (Horodatage de début)	`1159772400.0`	Heure de début de la requête en nombre de secondes à partir de l'ère.
`End Timestamp` (Horodatage de fin)	`1159858799.0`	Heure de fin de la requête en nombre de secondes à partir de l'ère.
`Begin Date` (Date de début)	`2006-10-02 07:00 GMT`	Date de début de la requête.
`End Date` (Date de fin)	`2006-10-03 06:59 GMT`	Date à laquelle la requête s'est terminée.
`Name` (Nom)	`(Nom)` (Logiciels publicitaires)	Nom de la catégorie de programmes malveillants.
`Transactions Monitored` (Transactions surveillées)	`525`	Nombre de transactions surveillées.
`Transactions Blocked` (Transactions bloquées)	`2100`	Nombre de transactions bloquées.
`Transactions Detected` (Transactions détectées)	`2625`	Nombre total de transactions = (Nombre de transactions détectées) + (Nombre de transactions bloquées).

Note – Les en-têtes de catégorie sont différents pour chaque type de rapport.

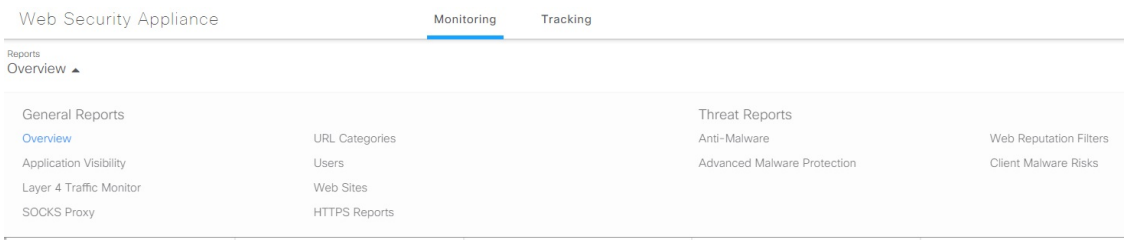
- Si vous exportez des données CSV localisées, il est possible que les en-têtes ne s'affichent correctement dans certains navigateurs. Cela se produit parce que certains navigateurs peuvent ne pas utiliser le jeu de caractères approprié pour le texte localisé. Pour contourner ce problème, vous pouvez enregistrer le fichier sur votre ordinateur local et l'ouvrir dans n'importe quel navigateur Web à l'aide de la commande **File > Open** (Fichier > Ouvrir). Lorsque vous ouvrez le fichier, sélectionnez le jeu de caractères pour afficher le texte localisé.

Utilisation des pages de rapport interactives sur la nouvelle interface Web

Vous pouvez afficher les rapports pour Secure Web Appliance à l'aide de la liste déroulante **Reports** (Rapports), comme le montre la figure suivante :

Remarque La page du rapport d'aperçu est la page de destination (la page affichée après la connexion). Le rechargement de la nouvelle interface Web à partir de n'importe quelle page de rapport ou de suivi charge la page de destination par défaut (page du rapport d'aperçu).

Illustration 10 : Liste déroulante des rapports



Les rapports Web peuvent être classés comme suit : **rapports généraux** et **rapports sur les menaces**.

Pour accéder à la nouvelle interface Web, consultez Rapports sur les appliances Secure sur la nouvelle interface Web.

Thèmes connexes

- (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458

Activation des rapports

Si votre organisation a plusieurs Secure Web Appliance et utilise une appliance Cisco de gestion de la sécurité de contenu pour gérer et afficher les données de rapports agrégées, vous devez activer les rapports centralisés sur chaque Secure Web Appliance.

Vous pouvez choisir le type de rapport en fonction de la configuration de l'appliance. Vous pouvez choisir de conserver tous les rapports localement. Si votre organisation a plusieurs Secure Web Appliance et qu'elle utilise une appliance Cisco Content Security Management, vous pouvez opter pour la production de rapports centralisés afin de gérer et d'afficher les données agrégées des rapports. Si vous choisissez les rapports centralisés ou les rapports locaux fournis , vous devez appliquer ces sélections sur chaque Secure Web Appliance.

Étape 1 Choisissez **Security Services** > **Reporting** (Services de sécurité > Rapports) et cliquez sur **Edit Settings** (Modifier les paramètres).

a) Sélectionnez **Local Reporting** (Rapports locaux) pour activer la création de rapports sur l'appliance. Les rapports seront accessibles après la connexion au portail de l'appliance.

b) Sélectionnez **Centralized Reporting** (Rapports centralisés) pour activer la création de rapports par l'intermédiaire de Cisco Content Security Management Appliance.

Secure Web Appliance ne stocke toutes ses données collectées que pour les rapports locaux. Si les rapports centralisés sont activés sur l'appliance, Secure Web Appliance ne conserve *que* les données de capacité et d'état du système, et ce sont les seuls rapports disponibles sur Secure Web Appliance localement.

Consultez la rubrique « Utilisation des rapports et du suivi centralisés du Web » dans le guide de l'utilisateur de votre Cisco Content Security Management Appliance pour en savoir plus sur la configuration de cette fonctionnalité sur l'appliance de gestion.

Étape 2 **Envoyez** et validez les modifications.

Planification des rapports

Vous pouvez planifier l'exécution de rapports sur une base quotidienne, hebdomadaire ou mensuelle. Les rapports planifiés peuvent être configurés pour inclure les données de la journée précédente, des sept jours précédents ou du mois précédent.

Vous pouvez planifier des rapports pour les types de rapports suivants :

- Survol
- Users (Utilisateurs)
- Sites Web
- URL Categories (Catégories d'URL)
- Visibilité de l'application
- Protection contre les programmes malveillants
- Cisco Secure Endpoint
- Mises à jour des verdicts Cisco Secure Endpoint
- Risques de programmes malveillants des clients
- Web Reputation Filters (Filtres de réputation Web)
- L4 Traffic Monitor (Supervision du trafic de la couche 4)
- Proxy SOCKS
- Rapports par emplacement d'utilisateur
- Capacité du système
- Mon tableau de bord

Ajout d'un rapport planifié

Étape 1 Choisissez **Reporting > Scheduled Reports** (Rapports > Rapports planifiés) et cliquez sur **Add Scheduled Report** (Ajouter un rapport planifié).

Étape 2 Choisissez un **Type** de rapport.

Étape 3 Entrez un **Titre** descriptif pour le rapport.

Évitez de créer plusieurs rapports sous le même nom.

Étape 4 Choisissez une plage de temps pour les données incluses dans le rapport.

Étape 5 Sélectionnez le **Format** du rapport généré.

Le format par défaut est PDF. La plupart des rapports vous permettent également d'enregistrer des données brutes dans un fichier CSV.

Étape 6 Selon le type de rapport que vous configurez, vous pouvez spécifier différentes options de rapport, telles que le nombre de lignes à inclure et la colonne selon laquelle trier les données. Configurez ces options selon vos besoins.

Étape 7 Dans la section **Schedule** (Planification), indiquez si vous souhaitez exécuter le rapport chaque jour, chaque semaine ou chaque mois, et à quelle heure.

Étape 8 Dans le champ **Email to** (Envoyer un e-mail à), saisissez les adresses de courriel auxquelles le rapport généré doit être envoyé.

Si vous n'indiquez pas d'adresse de messagerie, le rapport est simplement archivé.

Étape 9 Choisissez la **langue du rapport** pour les données.

Étape 10 Envoyez et validez les modifications.

Modification des rapports planifiés

Étape 1 Choisissez **Reporting > Scheduled Reports** (Rapports > Rapports planifiés).

Étape 2 Sélectionnez le titre du rapport dans la liste.

Étape 3 Modifiez les paramètres.

Étape 4 Envoyez et validez les modifications.

Suppression de rapports planifiés

Étape 1 Choisissez **Reporting > Scheduled Reports** (Rapports > Rapports planifiés).

Étape 2 Cochez les cases correspondant aux rapports que vous souhaitez supprimer.

Étape 3 Pour supprimer tous les rapports planifiés, cochez la case **All** (Tous).

Étape 4 **Supprimez** et **validez** les modifications.

Note Les versions archivées des rapports supprimés ne sont pas supprimées.

Création de rapports sur demande

Étape 1 Choisissez **Reporting > Archived Reports** (Rapports > Rapports archivés).

Étape 2 Cliquez sur **Generate Report Now** (Générer un rapport maintenant).

Étape 3 Choisissez un **Type** de rapport.

Étape 4 Entrez un **Titre** descriptif pour le rapport.

Évitez de créer plusieurs rapports sous le même nom.

Étape 5 Choisissez une plage de temps pour les données incluses dans le rapport.

Étape 6 Sélectionnez le **Format** du rapport généré.

Le format par défaut est PDF. La plupart des rapports vous permettent également d'enregistrer des données brutes dans un fichier CSV.

Étape 7 Selon le type de rapport que vous configurez, vous pouvez spécifier différentes options de rapport, telles que le nombre de lignes à inclure et la colonne selon laquelle trier les données. Configurez ces options selon vos besoins.

Étape 8 Sélectionnez une des **options de remise** :

- **Archivez** le rapport (il s'affichera dans la page des rapports archivés).
- **Envoyez maintenant le courriel aux destinataires**; indiquez une ou plusieurs adresses de courriel.

Étape 9 Choisissez la **langue du rapport** pour les données.

Étape 10 Cliquez sur **Deliver this Report** (Remettre ce rapport) pour générer le rapport.

Étape 11 Validez les modifications.

Rapports archivés

La page **Reporting > Archived Reports** (Rapports > Rapports archivés) répertorie les rapports archivés disponibles. Chaque nom dans la colonne Report Title (Titre du rapport) fournit un lien vers une vue de ce rapport. Le menu **Show** (Afficher) filtre les types de rapports répertoriés. Vous pouvez cliquer sur les en-têtes de colonne pour trier les données de chaque colonne.

L'appliance stocke jusqu'à 12 instances de chaque rapport planifié (jusqu'à 1000 rapports au total). Les rapports archivés sont stockés dans le répertoire `/PERODIC_reports` sur l'appliance. Les rapports archivés sont supprimés automatiquement. À mesure que de nouveaux rapports sont ajoutés, les anciens rapports sont supprimés pour maintenir le nombre à 1000. La limite de 12 instances s'applique à chaque rapport planifié du même nom et de la même plage de temps.

Résolution des problèmes liés aux rapports de supervision du trafic de la couche 4

Si le proxy Web est configuré comme un proxy de transfert et que l'option L4 Traffic Monitor (Supervision du trafic de la couche 4) est configurée pour surveiller tous les ports, l'adresse IP du port de données du proxy est enregistrée et affichée comme adresse IP du client dans les rapports. Si le proxy Web est configuré comme un proxy transparent, activez l'usurpation d'adresses IP pour enregistrer et afficher correctement les adresses IP des clients. Pour ce faire, consultez le Guide de l'utilisateur IronPort AsyncOS pour le Web.

Thèmes connexes

- Page Client Malware Risk (Risques de programmes malveillants des clients), on page 419
- Recherche de transactions traitées par la supervision du trafic de la couche 4 , on page 425

CHAPITRE 19

Rapports sur les appliances Secure

Cette rubrique contient les sections suivantes :

Page Overview (Survol)

La page **Reporting > Overview** (Rapports > Survol) fournit un synopsis de l'activité sur Secure Web Appliance. Elle contient des graphiques et des tableaux sommaires pour le trafic Web traité par Secure Web Appliance.

Table 7: Survol du système

Section	Description
Caractéristiques du trafic du proxy Web	Liste de la moyenne des transactions par seconde au cours de la dernière minute, de la bande passante moyenne (bit/s) au cours de la dernière minute, du temps de réponse moyen (ms) au cours de la dernière minute et du total des connexions actuelles.

Section	Description
Utilisation des ressources système	Liste de la `charge globale du processeur`, de `la RAM` et de l'utilisation `des disques pour les rapports et les` journaux. Cliquez sur **System Status Details** (Détails sur l'état du système) pour passer à la page System Status (État du système) (voir Page System Status (État du système) sur la nouvelle interface Web, on page 469 pour en savoir plus). **Note** La valeur d'utilisation du processeur affichée sur cette page et la valeur du processeur affichée sur la page System Status (État du système) peuvent différer légèrement, car elles sont lues séparément, à des moments différents.

Table 8: Catégories et résumés basés sur des plages de temps

Section	Description
Plage de temps : choisissez une plage de temps pour les données affichées dans les sections suivantes. Les options sont Hour (Heure), Day (Jour), Week (Semaine), 30 Days (30 jours), Yesterday (Hier) ou Custom Range (Plage personnalisée).	
Total Web Proxy Activity (Activité totale du proxy Web)	Affiche le nombre réel de transactions (échelle verticale) ainsi que la date approximative à laquelle l'activité (proxy Web) s'est produite (chronologie horizontale).
Web Proxy Summary (Résumé du proxy Web)	Vous permet d'afficher le pourcentage d'activités de proxy Web suspectes ou saines.
L4 Traffic Monitor Summary (Résumé de la supervision du trafic de la couche 4)	Rapports sur le trafic surveillé et bloqué par la supervision du trafic de la couche 4.
Suspect Transactions (Transactions suspectes)	Vous permet d'afficher les transactions Web qui ont été marquées comme suspectes par les divers composants de sécurité. Affiche le nombre réel de transactions ainsi que la date approximative à laquelle l'activité a eu lieu.
Suspect Transactions Summary (Résumé des transactions suspectes)	Vous permet d'afficher le pourcentage de transactions bloquées ou avec avertissement qui sont suspectes.
Top URL Categories: Total Transactions (Principales catégories d'URL : Total des transactions)	Affiche les 10 principales catégories d'URL qui ont été bloquées.
Top Application Types: Total Transactions (Principaux types d'application : Total des transactions)	
Top Malware Categories: Monitored or Blocked (Principales catégories de programmes malveillants : surveillés ou bloqués)	Affiche toutes les catégories de programmes malveillants qui ont été détectées.

Section	Description
Top Users: Blocked or Warned Transactions (Principaux utilisateurs : Transactions bloqués ou avec avertissement)	Affiche les utilisateurs qui génèrent les transactions bloquées ou avec avertissement. Les utilisateurs authentifiés sont affichés par nom d'utilisateur et les utilisateurs non authentifiés par adresse IP.
Web Traffic Tap Status (État de dérivation du trafic Web)	Affiche les transactions de trafic dérivé et non dérivé du trafic dans un format de graphique.
Web Traffic Tap Summary (Résumé des dérivations du trafic Web)	Affiche le résumé des transactions de trafic dérivé et non dérivé ainsi que le total des transactions de trafic.
Tapped HTTP/HTTPS Traffic (Trafic HTTP/HTTPS dérivé)	Affiche les transactions de trafic HTTP et HTTPS dérivé au format graphique.
Tapped Traffic Summary (Résumé du trafic dérivé)	Affiche le résumé des transactions de trafic HTTP et HTTPS ainsi que le total des transactions de trafic HTTP/HTTPS.
EUP Transactions (Transactions EUP)	Affiche les transactions URL encapsulées. Il s'agit de transactions effectuées par l'intermédiaire de sites Web comme *translate.google.com*.
EUP Transaction Summary (Résumé des transactions EUP)	Affiche le résumé des transactions d'URL encapsulées.
EUP Suspect Transactions (Transactions suspectes de EUP)	Affiche les transactions URL encapsulées qui se sont avérées suspectes.
EUP Suspect Transaction Summary (Résumé des transactions suspectes pour les EUP)	Affiche le résumé des transactions d'URL encapsulées jugées suspectes.

Page Users (Utilisateurs)

La page **Reporting > Users** (Rapports > Utilisateurs) fournit plusieurs liens qui vous permettent d'afficher les renseignements sur le trafic Web pour les utilisateurs individuels. Vous pouvez afficher le temps que les utilisateurs du réseau ont passé sur Internet, sur un site Web ou une URL en particulier, et la quantité de bande passante utilisée.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Top Users by Transactions Blocked (Principaux utilisateurs par transactions bloquées)	Répertorie les utilisateurs (échelle verticale) qui ont le plus grand nombre de transactions bloquées (échelle horizontale).

Top Users by Bandwidth Used (Principaux utilisateurs par bande passante utilisée)	Affiche les utilisateurs (échelle verticale) qui utilisent le plus de bande passante sur le système (échelle horizontale exprimée en gigaoctets).
Users Table (Tableau des utilisateurs)	Répertorie les utilisateurs individuels et affiche plusieurs statistiques pour chaque utilisateur.

Page User Details (Détails des utilisateurs)

La page **User Details** (Détails relatifs à l'utilisateur) affiche des informations sur un utilisateur spécifique sélectionné dans le tableau Users (Utilisateurs) de la page **Reporting > Users** (Rapports > Utilisateurs).

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
URL Categories by Total Transactions (Catégories d'URL par transactions totales)	Répertorie les catégories d'URL spécifiques utilisées par un utilisateur donné.
Trend by Total Transaction (Tendance par transaction totale)	Affiche l'heure à laquelle l'utilisateur a accédé au Web.
URL Categories Matched (Catégories d'URL correspondantes)	Affiche toutes les catégories d'URL correspondantes pendant une plage de temps spécifiée pour les transactions terminées et bloquées.
Domains Matched (Domaines correspondants)	Affiche des informations sur un domaine ou une adresse IP spécifique auquel cet utilisateur a accédé. **Note** Si vous exportez les données de ce domaine vers un fichier CSV, sachez que seules les 300 000 premières entrées seront exportées dans le fichier.
Applications Matched (Applications correspondantes)	
Malware Threats Detected (Programmes malveillants détectés)	Affiche les principaux programmes malveillants déclenchés par un utilisateur spécifique.
Policies Matched (Politiques correspondantes)	Affiche une politique spécifique appliquée à cet utilisateur en particulier.

Page User Count (Nombre d'utilisateurs)

La page **Reporting** > **User Count** (Rapports > Nombre d'utilisateurs) affiche des informations sur le nombre total d'utilisateurs authentifiés et non authentifiés sur l'appliance. La page répertorie le nombre d'utilisateurs uniques pour les 30, 90 et 180 derniers jours.

Remarque Le système calcule le nombre total d'utilisateurs authentifiés et non authentifiés une fois par jour.

Par exemple, si vous affichez le rapport sur le nombre d'utilisateurs au plus tard le 22 mai 23:59, le système affichera le nombre total d'utilisateurs jusqu'au 22 mai minuit.

Page Web Sites (Sites Web)

La page **Reporting > Web Sites** (Rapports > Sites Web) est une agrégation globale de l'activité qui se produit sur Secure Web Appliance.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Le menu vous permet de choisir la plage de temps des données contenues dans le rapport.
Top Domains by Total Transactions (Principaux domaines par total des transactions)	Répertorie les principaux domaines visités sur le site au format graphique.
Top Domains by Transactions Blocked (Principaux domaines par transactions bloquées)	Répertorie les principaux domaines qui ont déclenché une action de blocage par transaction au format graphique.
Domains Matched (Domaines correspondants)	Répertorie les domaines qui sont visités sur le site dans un tableau interactif. **Note** Si vous exportez les données de ce domaine vers un fichier CSV, sachez que seules les 300 000 premières entrées seront exportées dans le fichier.

Page URL Categories (Catégories d'URL)

La page **Reporting > URL Categories** (Rapports > Catégories d'URL) peut être utilisée pour afficher les catégories d'URL consultées par les utilisateurs sur le réseau. La page URL Categories (Catégories d'URL) peut être utilisée conjointement avec la page Application Visibility (Visibilité des applications) et la page Users (Utilisateurs) pour enquêter sur un utilisateur particulier ainsi que sur les types d'applications ou de sites Web auxquels un utilisateur particulier tente d'accéder.

Note L'ensemble de catégories d'URL prédéfinies est mis à jour occasionnellement.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport.
Top URL Categories by Total Transactions (Principales catégories d'URL par nombre total de transactions)	Cette section répertorie les principales catégories d'URL visitées sur le site au format graphique.
Top URL Categories by Blocked and Warned Transactions (Principales catégories d'URL par transactions bloquées et avec avertissement)	Répertorie les principales URL qui ont déclenché un blocage ou un avertissement par transaction au format graphique.
URL Categories Matched (Catégories d'URL correspondantes)	Affiche la disposition des transactions par catégorie d'URL pendant la plage de temps spécifiée, ainsi que la bande passante utilisée et le temps passé dans chaque catégorie. Si le pourcentage d'URL non classées est supérieur à 15 à 20 %, envisagez les options suivantes : • Pour des URL localisées précises, vous pouvez créer des catégories d'URL personnalisées et les appliquer à des utilisateurs ou à des groupes de politiques spécifiques. • Vous pouvez signaler les URL non classées et mal classées et à Cisco pour une évaluation et une mise à jour de la base de données. • Vérifiez que le filtrage de réputation Web et le filtrage contre les programmes malveillants sont activés.

Mises à jour et rapports des ensembles de catégories d'URL

L'ensemble de catégories d'URL prédéfinies peut être mis à jour régulièrement et automatiquement sur votre Secure Web Appliance.

Lorsque ces mises à jour se produisent, les noms des anciennes catégories continueront d'apparaître dans les rapports jusqu'à ce que les données associées aux anciennes catégories soient trop anciennes pour être incluses dans les rapports. Les données de rapport générées après la mise à jour d'un ensemble de catégories d'URL utiliseront les nouvelles catégories. Vous pouvez donc voir les anciennes catégories et les nouvelles dans le même rapport.

Page Application Visibility (Visibilité des applications)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Top Application Types by Total Transactions (Principaux types d'application par nombre total de transactions)	Cette section répertorie, au format graphique, les principaux types d'applications visitées sur le site.
Top Applications by Blocked Transactions (Principales applications par transactions bloquées)	Répertorie les principaux types d'applications qui ont déclenché un blocage par transaction au format graphique.
Application Types Matched (Types d'application correspondants)	Vous permet d'afficher des détails granulaires sur les types d'applications répertoriés dans le graphique Top Applications Type by Total Transactions (Types d'applications principales par total des transactions).
Applications Matched (Applications correspondantes)	Affiche toutes les applications pendant une plage de temps spécifiée.

Page Anti-Malware (Protection contre les programmes malveillants)

La page **Reporting > Anti-Malware** (Rapports > Protection contre les programmes malveillants) vous permet de surveiller et d'identifier les programmes malveillants détectés par le moteur Cisco DVS.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Top Malware Categories Detected (Principales catégories de programmes malveillants détectés)	Affiche les principales catégories de programmes malveillants détectées par le moteur DVS.
Top Malware Threats Detected (Principaux programmes malveillants détectés)	Affiche les principaux programmes malveillants détectés par le moteur DVS.
Malware Categories (Catégorie de programmes malveillants)	Affiche des informations sur des catégories particulières de programmes malveillants qui sont indiquées dans la section Top Malware Categories Detected (Principales catégories de programmes malveillants détectées).

Section	Description
Malware Threats (Programmes malveillants)	Affiche des informations sur des programmes malveillants particuliers qui sont indiqués dans la section Top Malware Threats (Principaux programmes malveillants).

Page Malware Category Report (Rapports sur les catégories de programmes malveillants)

Étape 1 Choisissez **Reporting > Anti-Malware** (Rapports > Protection contre les programmes malveillants).

Étape 2 Dans le tableau interactif Malware Categories (Catégories de programmes malveillants), cliquez sur une catégorie dans la colonne Malware Category (Catégorie de programmes malveillants).

Page Malware Threat Report (Rapport sur les menaces des programmes malveillants)

Étape 1 Choisissez **Reporting > Anti-Malware** (Rapports > Protection contre les programmes malveillants).

Étape 2 Dans le tableau Malware Threat (Programmes malveillants), cliquez sur une catégorie dans la colonne Malware Catégorie (Catégorie de programmes malveillants).

Page Cisco Secure Endpoint

Consultez Filtrage de réputation de fichiers et analyse de fichiers, on page 323.

Page File Analysis (Analyse des fichiers)

Consultez Création de rapports et suivi de la réputation et de l'analyse des fichiers , on page 340.

Page Cisco Secure Endpoint Verdict Updates (Mises à jour des verdicts Cisco Secure Endpoint

Consultez Filtrage de réputation de fichiers et analyse de fichiers, on page 323.

Consultez .

Page Client Malware Risk (Risques de programmes malveillants des clients)

La page **Reporting > Client Malware Risk** (Rapports > Risques liés aux programmes malveillants pour les clients) est une page de rapport sur la sécurité qui peut être utilisée pour surveiller les activités à risque des programmes malveillants pour les clients. La page Client Malware Risk (Risques liés aux programmes malveillants pour les clients) répertorie également les adresses IP des clients impliqués dans les connexions fréquentes de programmes malveillants, comme identifiées par la supervision du trafic de la couche 4 (L4TM).

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui vous permet de choisir la plage de temps des données contenues dans le rapport.
Web Proxy: Top Clients by Malware Risk (Proxy Web : Principaux clients par risque lié aux programmes malveillants)	Ce tableau affiche les dix principaux utilisateurs qui ont rencontré un risque lié à des programmes malveillants.
L4 Traffic Monitor: Malware Connections Detected (Supervision du trafic de la couche 4 : connexions à des programmes malveillants détectées)	Ce tableau affiche les adresses IP des ordinateurs de votre entreprise qui se connectent le plus souvent aux sites de programmes malveillants.
Web Proxy: Top Clients by Malware Risk (Proxy Web : Principaux clients par risque lié aux programmes malveillants)	Le tableau Web Proxy: Clients by Malware Risk (Proxy Web : clients par risque lié aux programmes malveillants) présente des informations détaillées sur des clients particuliers qui sont affichés dans la section Web Proxy: Top Clients by Malware Risk (Proxy Web : Principaux clients par risque lié aux programmes malveillants).
L4 Traffic Monitor: Clients by Malware Risk (Supervision du trafic de la couche 4 : clients par risque lié aux programmes malveillants)	Ce tableau affiche les adresses IP des ordinateurs de votre organisation qui se connectent fréquemment à des sites malveillants.

Page Client Detail (Détails des clients) pour le proxy Web – Clients par risque de programme malveillant

La page **Client Details** (Détails sur le client) affiche toutes les données sur l'activité Web et les risques liés aux programmes malveillants pour un client particulier au cours de la plage de temps spécifiée.

Étape 1 Choisissez **Reporting > Client Malware Risk** (Rapports > Risques liés aux programmes malveillants pour le client).

Étape 2 Dans la section **Web Proxy - Client Malware Risk** (Proxy Web > Risques liés aux programmes malveillants pour le client), cliquez sur un nom d'utilisateur dans la colonne « User ID/Client IP Address » (ID utilisateur/Adresse IP du client).

What to do next

Page User Details (Détails des utilisateurs), on page 414

Page Web Reputation Filters (Filtres de réputation Web)

La page **Reporting > Web Reputation Filters** (Rapports > Filtres de réputation Web) est une page de rapports liés à la sécurité qui vous permet d'afficher les résultats des filtres de réputation Web définis pour les transactions effectuées pendant une plage de temps spécifiée.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Web Reputation Actions (Trend) [Actions de réputation Web (tendance)]	Affiche le nombre total d'actions de réputation de sites Web (verticales) dans le temps spécifié (chronologie horizontale).
Web Reputation Actions (Volume) [Actions de réputation Web (volume)]	Affiche le volume d'actions de réputation Web en pourcentages par transaction.
Web Reputation Threat Types by Blocked Transactions (Types de menaces pour la réputation Web par transactions bloquées)	Affiche les types de menaces qui ont été bloquées en raison d'un faible score de réputation.
Web Reputation Threat Types by Scanned Further Transactions (Types de menaces pour la réputation Web par transactions supplémentaires analysées)	Affiche les types de menaces qui ont entraîné un score de réputation nécessitant l'analyse de la transaction.
Web Reputation Actions (Breakdown by Score) [Actions de réputation Web (répartition par score de réputation)]	Affiche les scores de réputation Web décomposés pour chaque action.

Page L4 Traffic Monitor (Supervision du trafic de la couche 4)

La page **Reporting> L4 Traffic Monitor** (Rapports > Supervision du trafic de la couche 4) est une page de rapports de sécurité qui affiche des informations sur les ports et les sites malveillants que le processus de supervision du trafic de la couche 4 a détectés au cours de la plage de temps spécifiée. Cette page affiche également les adresses IP des clients qui rencontrent fréquemment des sites malveillants.

La supervision du trafic de la couche 4 écoute le trafic réseau qui arrive par tous les ports de l'appliance et fait correspondre les noms de domaine et les adresses IP avec les entrées de ses propres tables de base de données pour déterminer s'il faut autoriser le trafic entrant et sortant.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui vous permet de choisir la plage de temps sur laquelle doit porter le rapport.
Top Client IPs (Principales adresses IP client)	Affiche, au format graphique, les adresses IP des ordinateurs de votre organisation qui se connectent le plus souvent aux sites malveillants.
Top Malware Sites (Principaux sites malveillants)	Affiche, au format graphique, les principaux domaines de programmes malveillants détectés par la supervision du trafic de la couche 4.
Client Source IPs (Adresses IP source client)	Affiche les adresses IP des ordinateurs de votre entreprise qui se connectent fréquemment à des sites malveillants.
Malware Ports (Ports de programmes malveillants)	Affiche les ports sur lesquels la supervision du trafic de la couche 4 a le plus souvent détecté des programmes malveillants.
Malware Sites Detected (Sites malveillants détectés)	Affiche les domaines dans lesquels la supervision du trafic de la couche 4 détecte le plus souvent des programmes malveillants.

Page SOCKS Proxy (Serveur mandataire SOCKS)

La page **Reporting > SOCKS Proxy** (Rapports > Serveur mandataire SOCKS) vous permet d'afficher les données et les tendances pour les transactions traitées par l'intermédiaire du mandataire SOCKS, notamment des informations sur les principales destinations et les principaux utilisateurs.

Page Reports by User Location (Rapports par emplacement des utilisateurs)

La page **Reporting > Reports by User Location** (Rapports > Rapports par emplacement d'utilisateur) vous permet de découvrir les activités de vos utilisateurs locaux et distants.

Les activités sont les suivantes :

- Catégories d'URL auxquelles accèdent les utilisateurs locaux et distants.
- Activité de la solution de protection contre les programmes malveillants déclenchée par les sites auxquels accèdent les utilisateurs locaux et distants.
- Réputation Web des sites consultés par les utilisateurs locaux et distants.
- Applications auxquelles les utilisateurs locaux et distants accèdent.
- Utilisateurs (locaux et distants).
- Domaines accessibles par les utilisateurs locaux et distants.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.

Section	Description
Total Web Proxy Activity: Remote Users (Activité totale du proxy Web : utilisateurs à distance)	Affiche l'activité de vos utilisateurs à distance (vertical) au cours de la période spécifiée (horizontal).
Web Proxy Summary (Résumé du proxy Web)	Affiche un résumé des activités des utilisateurs locaux et distants sur le réseau.
Total Web Proxy Activity: Local Users (Activité totale du proxy Web : utilisateurs locaux)	Affiche l'activité de vos utilisateurs à distance (vertical) au cours de la période spécifiée (horizontal).
Suspect Transactions Detected: Remote Users (Transactions suspectes détectées : utilisateurs à distance)	Affiche les transactions suspectes qui ont été détectées en raison des politiques d'accès définies pour les utilisateurs à distance (vertical) sur la période précisée (horizontal).
Suspect Transactions Summary (Résumé des transactions suspectes)	Affiche un résumé des transactions suspectes des utilisateurs à distance sur le réseau.
Suspect Transactions Detected: Local Users (Transactions suspectes détectées : utilisateurs locaux)	Affiche les transactions suspectes qui ont été détectées en raison des politiques d'accès définies pour vos utilisateurs à distance (vertical) au cours de la période spécifiée (horizontal).
Suspect Transactions Summary (Résumé des transactions suspectes)	Affiche un résumé des transactions suspectes des utilisateurs locaux sur le réseau.

Page Web Tracking (Suivi Web)

Utilisez la page de suivi Web pour rechercher et obtenir des détails sur des transactions individuelles ou des tendances de transactions qui peuvent être problématiques. Selon vos besoins, effectuez une recherche dans l'un des onglets suivants :

Page Web Tracking (Suivi Web)	Lien vers la tâche
Transactions processed by the Web Proxy (Transactions traitées par le proxy Web)	Recherche de transactions traitées par le proxy Web , on page 423
Transactions processed by the L4 Traffic Monitor (Transactions traitées par la supervision du trafic de la couche 4)	Recherche de transactions traitées par la supervision du trafic de la couche 4 , on page 425
Transactions processed by the SOCKS Proxy (Transactions traitées par le proxy SOCKS)	Recherche de transactions traitées par le serveur proxy SOCKS , on page 426

Vous pouvez également utiliser le nom de domaine complet pour rechercher des données de site Web dans la page **Web Tracking** (Suivi Web) pour certains cas, comme l'interconnexion transparente.

Note Une demande transparente affiche le nom du domaine ou du serveur sur la page de suivi. Cependant, lorsque des demandes transparentes, y compris l'intercommunication transparente, sont envoyées sans SNI, l'adresse IP est affichée.

Recherche de transactions traitées par le proxy Web

Vous pouvez utiliser l'onglet **Proxy Services** (Services proxy) sur la page **Reporting > Web Tracking** (Rapports > Suivi Web) pour suivre et produire un rapport sur l'utilisation du Web pour un utilisateur en particulier ou pour tous les utilisateurs.

Vous pouvez afficher les résultats de la recherche pour le type de transactions enregistrées (bloquées, surveillées, ayant fait l'objet d'un avertissement et terminées) pendant une période particulière. Vous pouvez également filtrer les résultats de données en utilisant plusieurs critères, tels que la catégorie d'URL, le programme malveillant et l'application.

Note Le proxy Web fournit uniquement des rapports sur les transactions qui comprennent une balise de décision ACL autre que OTHER-NONE.

Étape 1 Choisissez **Reporting > Web Tracking** (Rapports > Suivi Web).

Étape 2 Cliquez sur l'onglet **Proxy Services** (Services proxy).

Étape 3 Configurez les paramètres.

Paramètres	Description
Time Range (Plage de temps)	Choisissez la plage de temps sur laquelle porte le rapport.
IP de l'utilisateur ou du client	(Facultatif) Saisissez le nom d'utilisateur d'authentification tel qu'il apparaît dans les rapports ou une adresse IP du client que vous souhaitez suivre. Vous pouvez également saisir une plage d'adresses IP au format CIDR. Si vous laissez ce champ vide, la recherche renvoie des résultats pour tous les utilisateurs.
Website (Site Web)	(Facultatif) Saisissez un site Web que vous souhaitez suivre. Lorsque vous laissez ce champ vide, la recherche renvoie des résultats pour tous les sites Web. **Note** Vous pouvez rechercher les termes SNI (Server Name Indication). SNI, une extension du protocole TLS, permet aux clients de spécifier en toute sécurité des noms d'hôte lors de transactions Web. Vous devez spécifier des mots entiers. Pour que le SNI fonctionne, Cisco Secure Endpoint et les services de réputation doivent être activés.
Transaction Type (Type de transaction)	Choisissez le type de transactions que vous souhaitez suivre, soit All Transactions (Toutes les transactions), Completed (Terminé), Blocked (Bloqué), Monitored (Surpervisé) ou Warned (Ayant fait l'objet d'un avertissement).

Étape 4 (Facultatif) Développez la section Advanced (Avancé) et configurez les champs pour filtrer les résultats du suivi Web avec des critères plus avancés.

Paramètres	Description
URL Category (Catégorie URL)	Pour filtrer les données par catégorie d'URL, sélectionnez **Filter by URL Category** (Filtrer par catégorie d'URL) et saisissez la première lettre de la catégorie d'URL en fonction de laquelle effectuer le filtrage. Choisissez la catégorie dans la liste qui apparaît.
Application	Pour filtrer les données par application, sélectionnez **Filter by Application** (Filtrer par application) et choisissez une application en fonction de laquelle effectuer le filtrage. Pour filtrer les données par type d'application, sélectionnez **Filter by Application Type** (Filtrer par type d'application) et choisissez un type d'application selon lequel effectuer le filtrage.
Policy (Politique)	Pour filtrer les données par nom de la politique responsable de la décision finale pour cette transaction, sélectionnez **Filter by Action Policy** (Filtrer par politique d'action) et saisissez un nom de groupe de politiques [Access Policy (Politique d'accès), Decryption Policy (Politique de déchiffrement) ou Data Security Policy (Politique de sécurité des données)] selon lequel effectuer le filtrage. Consultez la description de PolicyGroupName dans la section Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500 pour de plus amples renseignements.
Cisco Secure Endpoint	Consultez À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint , on page 343.
Malware Threat (Programmes malveillants)	Pour filtrer les données par programme malveillant spécifique, sélectionnez **Filter by Malware Threat** (Filtrer par programme malveillant) et entrez le nom du programme malveillant selon lequel effectuer le filtrage. Pour filtrer les données par catégorie de programmes malveillants, sélectionnez **Filter by Malware Category** (Filtrer par catégorie de programmes malveillants) et choisissez une catégorie de programmes malveillants en fonction de laquelle effectuer le filtrage.
WBRS	Dans la section WBRS, vous pouvez filtrer les données par score de réputation de sites Web et par menace particulière pour la réputation de sites Web. • Pour filtrer les données par score de réputation Web, sélectionnez **Score range** (Plage de score de réputation), puis les valeurs supérieure et inférieure selon lesquelles effectuer le filtrage. Vous pouvez également filtrer les sites Web qui n'ont aucun score de réputation en sélectionnant **No Score** (Aucun score de réputation). • Pour filtrer les données par menace pour la réputation Web, sélectionnez **Filter by Reputation Threat** (Filtrer par menace pour la réputation) et saisissez une menace pour la réputation Web en fonction de laquelle effectuer le filtrage.
AnyConnect Secure Mobility	Pour filtrer les données selon l'emplacement des utilisateurs (distants ou locaux), sélectionnez **Filter by User Location** (Filtrer par emplacement des utilisateurs) et choisissez le type d'utilisateur selon lequel effectuer le filtrage.
User Request (Demande utilisateur)	Pour filtrer les données selon les transactions initiées par le client, sélectionnez **Filter by User-Demanded Transactions** (Filtrer selon les transactions demandées par l'utilisateur). **Note** Lorsque vous activez ce filtre, les résultats de la recherche incluent des transactions de type « meilleure estimation ».

Paramètres	Description
Encapsulated URL Protection (Protection encapsulée pour les URL)	Activez ce filtre pour les transactions URL encapsulées. **Note** • Vous devez activer le proxy HTTPS. Voir la section Activation du proxy HTTPS, on page 283. • Assurez-vous que la plage du score de réputation Web pour https://translate.google.com est définie sur decrypt (déchiffrer). Voir la section Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement, on page 316.

Étape 5 Cliquez sur **Search** (Recherche).

Les résultats sont triés par horodatage, le plus récent en premier.

Le nombre entre parenthèses sous le lien « Display Details » (Afficher les détails) désigne le nombre de transactions connexes générées par la transaction initiée par l'utilisateur, telles que les images chargées, les scripts javascript exécutés et les sites secondaires consultés.

Étape 6 (Facultatif) Cliquez sur **Display Details** (Afficher les détails) dans la colonne Transactions pour afficher des renseignements plus détaillés sur chaque transaction.

Note Si vous devez afficher plus de 1000 résultats, cliquez sur le lien de **Printable Download** (Téléchargement imprimable) pour obtenir un fichier CSV qui comprend l'ensemble complet des données brutes, à l'exclusion des détails des transactions connexes.

Tip Si une URL dans les résultats est tronquée, vous pouvez trouver l'URL complète dans le journal des accès.

Pour afficher les détails de jusqu'à 500 transactions connexes, cliquez sur le lien **Related Transactions** (Transactions connexes).

What to do next

- Mises à jour et rapports des ensembles de catégories d'URL , on page 416
- Descriptions des catégories de programmes malveillants, on page 321
- À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint , on page 343

Recherche de transactions traitées par la supervision du trafic de la couche 4

L'onglet L4 Traffic Monitor (Supervision du trafic de la couche 4) de la page **Reporting > Web Tracking** (Rapports > Suivi Web) fournit des détails sur les connexions aux ports et aux sites de programmes malveillants. Vous pouvez rechercher des connexions vers des sites de programmes malveillants à l'aide des types d'informations suivants :

- Plage de temps
- Site, utilisant l'adresse IP ou le domaine
- Port

- Adresse IP associée à un ordinateur au sein de votre organisation
- Type de connexion

Les 1000 premiers résultats de recherche correspondants s'affichent.

Recherche de transactions traitées par le serveur proxy SOCKS

Vous pouvez rechercher des transactions qui répondent à divers critères, notamment des transactions bloquées ou terminées; les utilisateurs; et le domaine de destination, l'adresse IP ou le port de destination.

Étape 1 Choisissez **Web > Reporting > Web Tracking** (Web > Rapports > Suivi Web).

Étape 2 Cliquez sur l'onglet **SOCKS Proxy** (Proxy SOCKS).

Étape 3 Pour filtrer les résultats, cliquez sur **Advanced** (Avancé).

Étape 4 Saisissez les critères de recherche.

Étape 5 Cliquez sur **Search** (Recherche).

What to do next

Page SOCKS Proxy (Serveur mandataire SOCKS) , on page 421

Page System Capacity (Capacité du système)

La page **Reporting > System Capacity** (Rapports > Capacité du système) affiche des informations actuelles et historiques sur l'utilisation des ressources dans la Secure Web Appliance.

Lors du choix des plages de temps pour l'affichage des données sur la page System Capacity (Capacité du système), il est important de vous rappeler les éléments suivants :

- **Hour Report** (Rapport horaire). Le rapport sur les heures interroge la table des minutes et affiche le nombre exact d'éléments, tels que les octets et la connexion, qui ont été enregistrés par l'appliance minute par minute sur une période de 60 minutes.
- **Day Report** (Rapport journalier). Le rapport journalier interroge la table des heures et affiche le nombre exact d'éléments, tels que les octets et la connexion, qui ont été enregistrés par l'appliance sur une base horaire pendant une période de 24 heures. Ces informations sont recueillies à partir de la table des heures.

Le rapport hebdomadaire et le rapport sur 30 jours fonctionnent de manière similaire aux rapports horaire et journalier.

Page System Status (État du système)

Utilisez la page **Reporting> System Status** (Rapports > État du système) pour surveiller l'état du système. Cette page affiche l'état et la configuration actuels de Secure Web Appliance.

Cette section...	Écrans
État Secure Web Appliance	• Disponibilité du système • Utilisation des ressources système : utilisation du processeur, de la RAM et pourcentage d'espace disque utilisé pour les rapports et la journalisation. La valeur d'utilisation du processeur affichée sur cette page et la valeur du processeur affichée sur la page de présentation du système (Page Overview (Survol), on page 411) peuvent différer légèrement, car elles sont lues séparément, à des moments différents. L'utilisation de la RAM pour un système qui fonctionne efficacement peut être supérieure à 90 %, car la RAM qui n'est pas autrement utilisée par le système est utilisée par le cache d'objets Web. Si votre système ne connaît pas de problèmes de performances graves et que cette valeur n'est pas bloquée à 100 %, le système fonctionne normalement. **Note** La mémoire tampon du proxy est un composant qui utilise cette RAM.
Proxy Traffic Characteristics (Caractéristiques du trafic du proxy)	• Transactions par seconde • Bande passante • Temps de réponse • Ratio de résultats du cache • Connexions
Dérivation du trafic Web	Utilisation du processeur de dérivation du trafic Web.
High Availability (Haute disponibilité)	État du service à haute disponibilité.
Services externes	• Identity Service Engine (ISE)

Cette section...	Écrans
Configuration actuelle	Paramètres du proxy Web : • Web Proxy Status (État du proxy Web) : activé ou désactivé. • Deployment Topology (Topologie du déploiement). • Web Proxy Mode (Mode du proxy Web) : direct ou transparent. • IP Spoofing (Usurpation d'adresses IP) : activée ou désactivée. Paramètres de supervision du trafic de la couche 4 : • L4 Traffic Monitor Status (État de la supervision du trafic de la couche 4) : activé ou désactivé. • L4 Traffic Monitor Wiring (Câblage pour la supervision du trafic de la couche 4). • L4 Traffic Monitor Action (Action de supervision du trafic de la couche 4) : superviser ou bloquer. Paramètres de dérivation du trafic Web : • Web Traffic Tap Status (État de la dérivation du trafic Web) : activé ou désactivé • Web Traffic Tap Interface (Interface de dérivation du trafic Web) : P1, P2, TI ou T2 Information de version de Secure Web Appliance Informations sur le matériel

Thèmes connexes

Page System Capacity (Capacité du système), on page 426

CHAPITRE 20

Rapports sur les appliances Secure sur la nouvelle interface Web

Cette rubrique contient les sections suivantes :

Interprétation des pages de rapports Web sur la nouvelle interface Web

Le tableau suivant répertorie les rapports dans le menu déroulant Reports (Rapports). Cette option est disponible dans la dernière version prise en charge d'AsyncOS pour les Secure Web Appliance dans la liste déroulante **Reports** (Rapports) de l'interface Web. Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406. Si vos Secure Web Appliance exécutent des versions antérieures d'AsyncOS, tous ces rapports ne sont pas disponibles.

Tableau 9 : Options de la liste déroulante Web Reports (Rapports Web)

Option de liste déroulante Reports (Rapports)	Action
General Reports (Rapports généraux)	
Page Overview (Survol)	La page de survol fournit un résumé de l'activité de vos Secure Web Appliance. Elle contient des graphiques et des tableaux récapitulatifs pour les transactions entrantes et sortantes. Pour obtenir plus d'informations, reportez-vous à la section Page Overview (Survol), à la page 433.

Option de liste déroulante Reports (Rapports)	Action
Page Application Visibility (Visibilité des applications)	La page Application Visibility (Visibilité des applications) vous permet d'appliquer et d'afficher les contrôles qui ont été appliqués à un type d'application particulier dans l'appliance de gestion de la sécurité et Secure Web Appliance. Pour obtenir plus d'informations, reportez-vous à la section Page Application Visibility (Visibilité des applications), à la page 434.
Page Layer 4 Traffic Monitor (Supervision du trafic de la couche 4)	Vous permet d'afficher les informations sur les ports et les sites malveillants que la supervision du trafic de la couche 4 a détectés au cours de la plage de temps spécifiée. Pour obtenir plus d'informations, reportez-vous à la section Page Layer 4 Traffic Monitor (Supervision du trafic de la couche 4), à la page 436.
Page SOCKS Proxy (Serveur mandataire SOCKS)	Vous permet d'afficher les données des transactions de mandataire SOCKS, notamment les destinations et les utilisateurs. Pour obtenir plus d'informations, reportez-vous à la section Page SOCKS Proxy (Serveur mandataire SOCKS), à la page 439.
Page URL Categories (Catégories d'URL)	La page URL Categories (Catégories d'URL) vous permet d'afficher les principales catégories d'URL consultées, notamment : • Principales URL qui ont déclenché un blocage ou un avertissement par transaction. • Toutes les catégories d'URL au cours d'une plage de temps spécifiée pour les transactions terminées, ayant fait l'objet d'un avertissement et bloquées. Il s'agit d'un tableau interactif contenant des en-têtes de colonne interactifs que vous pouvez utiliser pour trier les données selon vos besoins. Pour obtenir plus d'informations, reportez-vous à la section Page URL Categories (Catégories d'URL), à la page 440.

Option de liste déroulante Reports (Rapports)	Action
Page Users (Utilisateurs)	La page Users (Utilisateurs) fournit plusieurs liens de suivi Web qui vous permettent d'afficher les renseignements de suivi Web pour chaque utilisateur. Dans la page Users (Utilisateurs), vous pouvez voir combien de temps un ou plusieurs utilisateurs de votre système ont passé sur Internet, sur un site ou une URL particulier, et la quantité de bande passante utilisée par ces utilisateurs. Dans la page Users (Utilisateurs), vous pouvez cliquer sur un utilisateur individuel dans le tableau interactif Users (Utilisateurs) pour afficher plus de détails sur cet utilisateur en particulier dans la page User Details (Détails sur l'utilisateur). La page User Details (Détails sur l'utilisateur) vous permet de voir des renseignements précis sur un utilisateur que vous avez identifié dans le tableau Users (Utilisateurs) de la page Users (Utilisateurs). Dans cette page, vous pouvez enquêter sur l'activité de chaque utilisateur sur votre système. Cette page est particulièrement utile si vous effectuez des enquêtes au niveau de l'utilisateur et que vous avez besoin de savoir, par exemple, quels sites vos utilisateurs visitent, à quelles menaces liées à des programmes malveillants ils sont confrontés, à quelles catégories d'URL ils accèdent et combien de temps un utilisateur spécifique passe sur ces sites. Pour obtenir plus d'informations, reportez-vous à la section Page Users (Utilisateurs), à la page 445. Pour en savoir plus sur un utilisateur spécifique de votre système, consultez Page User Details (Détails des utilisateurs) (Web Reporting [Création de rapports Web]) , à la page 446.
Page Web Sites (Sites Web)	La page Web Sites (Sites Web) vous permet d'afficher une agrégation globale de l'activité qui se produit sur vos appliances gérées. Cette page vous permet de surveiller les sites Web à risque élevé consultés pendant une plage de temps précise. Pour obtenir plus d'informations, reportez-vous à la section Page Web Sites (Sites Web), à la page 449.
HTTPS Reports (Rapports HTTPS)	La page HTTPS Reports (Rapports HTTPS) est une agrégation globale du résumé du trafic HTTP/HTTPS (transactions ou utilisation de la bande passante) sur les appliances gérées. Pour plus d'information, consultez Page HTTPS Reports (Rapports HTTPS), à la page 443
Threat Reports (Rapport sur les menaces)	

Option de liste déroulante Reports (Rapports)	Action
Page Anti-Malware (Protection contre les programmes malveillants)	La page Anti-Malware (Protection contre les programmes malveillants) vous permet d'afficher les informations sur les ports et les sites malveillants que les moteurs d'analyse de protection contre les programmes malveillants ont détectés au cours de la plage de temps spécifiée. La partie supérieure du rapport affiche le nombre de connexions pour chacun des principaux ports et sites Web malveillants. La partie inférieure du rapport affiche les ports et les sites malveillants détectés. Pour obtenir plus d'informations, reportez-vous à la section Page Anti-Malware (Protection contre les programmes malveillants), à la page 451.
Page Cisco Secure Endpoint	Cisco Secure Endpoint vous protège contre les menaces « jour zéro » et les menaces basées sur les fichiers en obtenant la réputation des fichiers connus, en analysant le comportement de certains fichiers qui ne sont pas encore connus du service de réputation, en évaluant continuellement les menaces émergentes à mesure que de nouvelles informations sont disponibles, et en vous informant sur les fichiers qui sont considérées comme des menaces après leur entrée dans votre réseau. Pour en savoir plus, consultez Page Cisco Secure Endpoint, à la page 450.
Page Client Malware Risk (Risques de programmes malveillants des clients)	La page Client Malware Risk (Risques de programmes malveillants des clients) est une page de rapports liés à la sécurité qui peut être utilisée pour identifier les ordinateurs clients qui peuvent se connecter de manière inhabituelle à des sites malveillants. Pour obtenir plus d'informations, reportez-vous à la section Page relative aux risques des programmes malveillants du client, à la page 455.
Page Web Reputation Filters (Filtres de réputation Web)	Vous permet d'afficher les rapports sur le filtrage de réputation Web pour les transactions effectuées pendant une plage de temps spécifiée. Pour obtenir plus d'informations, reportez-vous à la section Page Web Reputation Filters (Filtres de réputation Web), à la page 456.

À propos du temps passé

La colonne Time Spent (Temps passé) de divers tableaux représente le temps qu'un utilisateur a passé sur une page Web. Aux fins d'enquête sur un utilisateur, le temps passé par l'utilisateur sur chaque catégorie d'URL. Lors du suivi d'une URL, le temps passé par chaque utilisateur sur cette URL spécifique.

Une fois qu'un événement de transaction est balisé comme « vu », c'est-à-dire qu'un utilisateur accède à une URL particulière, une valeur de « Temps passé » commencera à être calculée et ajoutée en tant que champ du tableau de rapport Web.

Pour calculer le temps nécessaire, AsyncOS affecte à chaque utilisateur actif 60 secondes d'activité pendant une minute. À la fin de la minute, le temps passé par chaque utilisateur est réparti uniformément entre les différents domaines visités par l'utilisateur. Par exemple, si un utilisateur se connecte à quatre domaines différents en une minute d'activité, on considère que l'utilisateur a passé 15 secondes sur chaque domaine.

Aux fins de la valeur du temps passé, examinons les remarques suivantes :

- Un utilisateur actif est défini comme un nom d'utilisateur ou une adresse IP qui envoie le trafic HTTP par l'intermédiaire de l'appliance et a accédé à un site Web qu'AsyncOS considère comme une « consultation de page ».
- AsyncOS définit une page consultée comme une requête HTTP initiée par l'utilisateur, par opposition à une requête initiée par l'application client. AsyncOS utilise un algorithme heuristique pour deviner au mieux d'identifier les pages des utilisateurs.

Les unités sont affichées au format Heures:Minutes.

Page Overview (Survol)

La page du rapport **Survol** fournit un résumé de l'activité de vos Secure Web Appliance. Elle contient des graphiques et des tableaux récapitulatifs pour les transactions entrantes et sortantes.

Pour afficher la page du rapport d'aperçu, choisissez **Monitoring > Overview** (Supervision > Survol) d'ensemble dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

De manière générale, la page du rapport **Overview** (Survol) présente des statistiques sur l'utilisation de l'URL et des utilisateurs, l'activité du proxy Web et divers résumés des transactions. Les résumés des transactions vous donnent plus de détails sur les tendances, par exemple, les transactions suspectes et, en face de ce graphique, combien de ces transactions suspectes sont bloquées et la manière dont elles sont bloquées.

L'utilisation est réservée à la moitié inférieure de la page du rapport d'aperçu. À savoir, les principales catégories d'URL affichées, les principaux types et catégories d'applications bloquées et les principaux utilisateurs qui génèrent ces blocages ou avertissements.

Tableau 10 : Détails sur la page de survol

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Total Web Proxy Activity (Activité totale du proxy Web)	Vous pouvez afficher l'activité du proxy Web signalée par les Secure Web Appliance actuellement gérés par l'appliance de gestion de la sécurité. Cette section affiche le nombre réel de transactions et la date approximative à laquelle l'activité s'est produite au format graphique. Vous pouvez également afficher le pourcentage d'activités de proxy Web qui sont suspectes ou d'activités de proxy saines, notamment le nombre total de transactions.

Section	Description
Suspect Transactions (Transactions suspectes)	Vous pouvez afficher les transactions Web que l'administrateur a marquées comme suspectes au format graphique. Cette section affiche le nombre réel de transactions et la date approximative à laquelle l'activité a eu lieu au format graphique. Vous pouvez également afficher le pourcentage de transactions bloquées ou avec avertissement qui sont suspectes. En outre, vous pouvez voir le type de transactions qui ont été détectées et bloquées et le nombre réel de fois que ces transactions ont été bloquées.
L4 Traffic Monitor Summary (Résumé de la supervision du trafic de la couche 4)	Vous pouvez afficher tout trafic de la couche 4 signalé par les Secure Web Appliance qui sont actuellement gérés par l'appliance de gestion de la sécurité au format graphique.
Top URL Categories: Total Transactions (Principales catégories d'URL : Total des transactions)	Vous pouvez afficher les principales catégories d'URL qui sont bloquées, y compris le type de catégorie d'URL et le nombre réel de fois que le type spécifique de catégorie a été bloqué, au format graphique. L'ensemble de catégories d'URL prédéfinies est mis à jour occasionnellement. Pour plus d'informations sur l'incidence de ces mises à jour sur les résultats des rapports, consultez Mises à jour et rapports des ensembles de catégories d'URL , à la page 442.
Top Application Types: Total Transactions (Principaux types d'application : Total des transactions)	Vous pouvez afficher au format graphique les principaux types d'applications bloquées, notamment le nom du type d'application réel et le nombre de fois que l'application a été bloquée.
Top Malware Categories: Monitored or Blocked (Principales catégories de programmes malveillants : surveillés ou bloqués)	Vous pouvez afficher toutes les catégories de programmes malveillants qui ont été détectées au format graphique.
Top Users: Blocked or Warned Transactions (Principaux utilisateurs : Transactions bloqués ou avec avertissement)	Vous pouvez afficher les utilisateurs réels qui génèrent les transactions bloquées ou avec avertissement au format graphique. Les utilisateurs peuvent être affichés par adresse IP ou par nom d'utilisateur.
Top Threat Categories: Blocked by WBRS (Principales catégories de menaces : blocage par WBRS)	Vous pouvez afficher toutes les catégories de menaces qui ont été bloquées au format graphique

Page Application Visibility (Visibilité des applications)

Remarque Pour des informations détaillées sur Application Visibility, consultez la rubrique « Comprendre Application Visibility and Control » dans le Guide de l'utilisateur d'AsyncOS pour Cisco Secure Web Appliance.

La page du rapport **Application Visibility** (Visibilité des applications) vous permet d'appliquer des contrôles à des types d'applications particuliers dans l'appliance de gestion de la sécurité et Secure Web Appliance.

Pour afficher la page de rapport sur la visibilité des applications, choisissez **Monitoring > Application Visibility** (Supervision > Visibilité des applications) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Le contrôle des applications vous donne un contrôle plus granulaire sur le trafic Web que le simple filtrage d'URL, par exemple, ainsi qu'un meilleur contrôle sur les types d'application suivants :

- Les applications de contournement, comme les anonymiseurs et les tunnels chiffrés.
- Des applications de collaboration, comme Cisco Webex, Facebook et la messagerie instantanée.
- Les applications exigeantes en ressources, comme la diffusion de données multimédias en continu.

Comprendre la différence entre les applications et les types d'application

Il est essentiel de comprendre la différence entre une application et un type d'application afin de pouvoir contrôler les applications utilisées pour vos rapports.

- **Application Types** (Types d'application). Catégorie qui contient une ou plusieurs applications. Par exemple, les moteurs de recherche sont un type d'application qui peut contenir des moteurs de recherche tels que Google Search et Craigslist. La messagerie instantanée est une autre catégorie de type d'application qui peut contenir Yahoo Instant Messenger ou Cisco WebEx. Facebook est également un type d'application.
- **Applications**. Applications particulières qui appartiennent à un type d'application. Par exemple, YouTube est une application de type application multimédia.
- **Application behaviors** (Comportements des applications). Actions ou comportements particuliers que les utilisateurs peuvent accomplir dans une application. Par exemple, les utilisateurs peuvent transférer des fichiers tout en utilisant une application telle que Yahoo Messenger. Toutes les applications n'incluent pas des comportements d'application que vous pouvez configurer.

Remarque Pour des informations détaillées sur la façon d'utiliser le moteur Application Visibility and Control (AVC) pour contrôler l'activité de Facebook, consultez la rubrique « Comprendre la visibilité et le contrôle des applications » dans le guide de l'utilisateur d'AsyncOS pour Cisco Secure Web Appliance.

La page Application Visibility (Visibilité des applications) vous permet d'afficher les informations suivantes :

Tableau 11 : Détails indiqués sur la page Application Visibility (Visibilité des applications)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.

Section	Description
Top Application Types by Total Transactions (Principaux types d'application par nombre total de transactions)	Vous pouvez afficher les principaux types d'applications visités sur le site au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458. Par exemple, les outils de messagerie instantanée tels que les types d'applications Yahoo Instant Messenger, Facebook et Presentation.
Top Applications by Blocked Transactions (Principales applications par transactions bloquées)	Vous pouvez afficher les principaux types d'application qui ont déclenché un blocage par transaction au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458. Par exemple, un utilisateur a essayé de démarrer un certain type d'application, par exemple Google Talk ou Yahoo Instant Messenger, et en raison d'une politique spécifique en place, une action de blocage a été déclenchée. Cette application est ensuite répertoriée dans ce graphique en tant que transaction bloquée ou avertissement.
Application Types Matched (Types d'application correspondants)	Le tableau interactif Application Types Matched (Types d'applications correspondants) vous permet d'afficher des détails granulaires sur les types d'application répertoriés dans le tableau Top Applications Type by Total Transactions (Principaux types d'applications par total des transactions). Dans la colonne Applications, vous pouvez cliquer sur une application pour en afficher les détails.
Applications Matched (Applications correspondantes)	Le tableau interactif Applications Matched (Applications correspondantes) affiche toutes les applications pendant une plage de temps spécifiée. En outre, vous pouvez trouver une application précise dans la section Application Matched (Application correspondante). Dans le champ de texte au bas de cette section, saisissez le nom de l'application spécifique et cliquez sur Find Application (Rechercher une application).

Page Layer 4 Traffic Monitor (Supervision du trafic de la couche 4)

La page du rapport **Layer 4 Traffic Monitor** (Supervision du trafic de la couche 4) affiche des informations sur les ports et les sites malveillants que la supervision du trafic de la couche 4 sur vos Secure Web Appliance a détectés au cours de la plage de temps spécifiée. Cette page affiche également les adresses IP des clients qui rencontrent fréquemment des sites malveillants.

Pour afficher la page de rapport sur les sites Web, sélectionnez **Monitoring > Web Sites** (Supervision >Sites Web) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

La supervision du trafic de la couche 4 écoute le trafic réseau qui arrive par tous les ports de chaque Secure Web Appliance et fait correspondre les noms de domaine et les adresses IP avec les entrées de ses propres tables de base de données pour déterminer s'il faut autoriser le trafic entrant et sortant.

Vous pouvez utiliser les données de ce rapport pour déterminer s'il faut bloquer un port ou un site ou pour analyser pourquoi une adresse IP client particulière se connecte anormalement fréquemment à un site malveillant (par exemple, cela peut être parce que l'ordinateur associé à cette adresse IP est infecté par un programme malveillant qui tente de se connecter à un serveur de commande et de contrôle central).

Tableau 12 : Page de détails sur la page Layer 4 Traffic Monitor (Supervision du trafic de la couche 4)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Top Client IPs: Malware Connections Detected (Principales adresses IP de clients : connexions de programmes malveillants détectées)	Vous pouvez afficher les principales adresses IP des ordinateurs de votre organisation qui se connectent le plus souvent à des sites malveillants, au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. Pour en savoir plus, consultez Choix des données à représenter au format graphique , à la page 403. Ce tableau est identique au tableau « Layer 4 Traffic Monitor: Malware Connections Detected » (Supervision du trafic de la couche 4 : connexions malveillantes détectées) dans Page relative aux risques des programmes malveillants du client, à la page 455.
Top Malware Sites: Malware Connections Detected (Principaux sites malveillants : connexions de programmes malveillants détectées)	Vous pouvez afficher les principaux domaines de programmes malveillants détectés par la supervision du trafic de la couche 4, au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. Pour en savoir plus, consultez Choix des données à représenter au format graphique , à la page 403.

Section	Description
Client Source IPs (Adresses IP source client)	Vous pouvez utiliser ce tableau interactif pour afficher les adresses IP des ordinateurs de votre organisation qui se connectent fréquemment à des sites malveillants. Pour inclure uniquement les données d'un port en particulier, entrez un numéro de port dans la case au bas du tableau et cliquez sur Filter by Client IP(Filtrer par adresse IP de client). Vous pouvez utiliser cette fonctionnalité pour déterminer les ports utilisés par les programmes malveillants qui « renvoient à la source » des sites malveillants. Pour afficher des détails tels que le port et le domaine de destination de chaque connexion, cliquez sur une entrée dans le tableau. Par exemple, si l'adresse IP d'un client en particulier a un nombre élevé de connexions de programmes malveillants bloquées, cliquez sur le nombre dans cette colonne pour afficher la liste de chaque connexion bloquée. La liste s'affiche en tant que résultats de recherche dans l'onglet Layer 4 Traffic Monitor (Supervision du trafic de la couche 4) de la page de recherche de suivi Web. Pour plus d'informations sur cette liste, consultez Recherche de transactions traitées par la supervision du trafic de la couche 4, à la page 464. Ce tableau est identique au tableau « Layer 4 Traffic Monitor: Malware Connections Detected » (Supervision du trafic de la couche 4 : connexions malveillantes détectées) dans Page relative aux risques des programmes malveillants du client, à la page 455.
Malware Ports (Ports de programmes malveillants)	Vous pouvez utiliser ce tableau interactif pour afficher les ports sur lesquels la supervision du trafic de la couche 4 a le plus souvent détecté des programmes malveillants. Pour afficher les détails, cliquez sur une entrée dans le tableau. Par exemple, cliquez sur le nombre total de connexions malveillantes détectées pour afficher les détails concernant chaque connexion sur ce port. La liste s'affiche en tant que résultats de recherche dans l'onglet Layer 4 Traffic Monitor (Supervision du trafic de la couche 4) de la page de recherche de suivi Web. Pour plus d'informations sur cette liste, consultez Recherche de transactions traitées par la supervision du trafic de la couche 4, à la page 464.

Section	Description
Malware Sites Detected (Sites malveillants détectés)	Vous pouvez utiliser ce tableau interactif pour afficher les domaines dans lesquels la supervision du trafic de la couche 4 détecte le plus souvent des programmes malveillants. Pour inclure uniquement les données d'un port en particulier, entrez un numéro de port dans le champ au bas du tableau et cliquez sur Filter by Port (Filtrer par port). Vous pouvez utiliser cette fonctionnalité pour déterminer s'il faut bloquer un site ou un port. Pour afficher les détails, cliquez sur une entrée dans le tableau. Par exemple, cliquez sur le nombre de connexions malveillantes bloquées pour afficher la liste de chaque connexion bloquée pour un site en particulier. La liste s'affiche en tant que résultats de recherche dans l'onglet Layer 4 Traffic Monitor (Supervision du trafic de la couche 4) de la page de recherche de suivi Web. Pour plus d'informations sur cette liste, consultez Recherche de transactions traitées par la supervision du trafic de la couche 4, à la page 464.

Thèmes connexes

Résolution des problèmes liés aux rapports de supervision du trafic de la couche 4 , à la page 410

Page SOCKS Proxy (Serveur mandataire SOCKS)

La page du rapport SOCKS Proxy (Serveur mandataire SOCKS) vous permet d'afficher les transactions traitées par le biais du mandataire SOCKS, y compris les informations sur les destinations et les utilisateurs, au format graphique et tabulaire.

Pour afficher la page de rapport sur le proxy SOCKS, sélectionnez **Monitoring > SOCKS Proxy** (Supervision > SOCKS Proxy) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Remarque La destination indiquée dans le rapport est l'adresse que le client SOCKS (généralement un navigateur) envoie au serveur proxy SOCKS.

Pour modifier les paramètres de politique SOCKS, consultez le *Guide de l'utilisateur pour AsyncOS pour Cisco Secure Web Appliance*.

Tableau 13 : Détails sur la page SOCKS Proxy (Serveur mandataire SOCKS)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.

Section	Description
Top Destinations for SOCKS: Total Transactions (Principales destinations pour SOCKS : Total des transactions)	Vous pouvez afficher les principales destinations détectées par le proxy SOCKS au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Top Users for SOCKS: Malware Transactions (Principaux utilisateurs pour SOCKS : Transactions malveillantes)	Vous pouvez afficher les principaux utilisateurs détectés par le proxy SOCKS au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Destinations	Vous pouvez utiliser ce tableau interactif pour afficher la liste des domaines de destination ou des adresses IP traités par le biais du proxy SOCKS. Pour inclure uniquement les données relatives à une destination particulière, entrez un nom de domaine ou une adresse IP dans la zone au bas du tableau, puis cliquez sur **Find Domain or IP** (Rechercher un domaine ou une adresse IP).
Users (Utilisateurs)	Vous pouvez utiliser ce tableau interactif pour afficher la liste des utilisateurs ou des adresses IP traitées par le biais du proxy SOCKS. Pour inclure uniquement les données d'un utilisateur en particulier, entrez un nom d'utilisateur ou une adresse IP dans la zone au bas du tableau et cliquez sur **Find User ID/Client IP Address** (Rechercher l'ID utilisateur /l'adresse IP du client).

Thèmes connexes

Recherche de transactions traitées par le serveur proxy SOCKS , à la page 464

Page URL Categories (Catégories d'URL)

La page de rapport **URL Categories** (Catégories d'URL) permet d'afficher les catégories d'URL des sites que les utilisateurs sur votre système visitent.

Pour afficher la page de rapport sur les catégories d'URL, choisissez **Monitoring > URL Categories** (Supervision > Catégories d'URL) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Vous pouvez afficher les informations suivantes dans la page URL Categories (Catégories d'URL) :

Tableau 14 : Détails sur la page des catégories d'URL

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Top URL Categories: Total Transactions (Principales catégories d'URL : Total des transactions)	Vous pouvez afficher les principales catégories d'URL visitées sur le site au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Top URL Categories: Blocked and Warned Transactions (Principales catégories d'URL : Transactions bloquées et avec avertissement)	Vous pouvez afficher les principales URL qui ont déclenché un blocage ou un avertissement par transaction au format graphique. Par exemple, un utilisateur a accédé à une URL particulière et, en raison d'une politique spécifique en place, cela a déclenché une action de blocage ou un avertissement. Cette URL est ensuite répertoriée dans ce graphique en tant que transaction bloquée ou avertissement. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Top Youtube Categories : Total Transactions (Principales catégories Youtube : Total des transactions)	Vous pouvez afficher les principales catégories YouTube visitées sur le site au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Top Youtube Categories : Blocked and Warned Transactions (Principales catégories YouTube : transactions bloquées et avec avertissement)	Vous pouvez afficher les principales URL YouTube qui ont déclenché un blocage ou un avertissement par transaction au format graphique. Par exemple, un utilisateur a accédé à une URL YouTube particulière et, en raison d'une politique spécifique en place, cela a déclenché une action de blocage ou un avertissement. Cette URL YouTube est ensuite répertoriée dans ce graphique en tant que transaction bloquée ou avertissement. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.

Section	Description
URL Categories Matched (Catégories d'URL correspondantes)	Le tableau interactif correspondant aux catégories d'URL affiche la disposition des transactions par catégorie d'URL pendant la plage de temps spécifiée, ainsi que la bande passante utilisée et le temps passé dans chaque catégorie. S'il y a un grand nombre d'URL non classées, consultez Réduction des URL non classées , à la page 442.

Réduction des URL non classées

Si le pourcentage d'URL non classées est supérieur à 15 à 20 %, envisagez les options suivantes :

- Pour des URL localisées précises, vous pouvez créer des catégories d'URL personnalisées et les appliquer à des utilisateurs ou à des groupes de politiques spécifiques. Ces transactions seront ensuite incluses dans les statistiques « URL Filtering Bypassed » (Filtrage d'URL contourné). Pour ce faire, consultez les informations sur les catégories d'URL personnalisées dans le Guide de l'utilisateur d'AsyncOS pour Cisco Secure Web Appliance.
- Pour connaître les sites qui devraient être inclus dans les catégories existantes ou autres, consultez Signalisation des URL mal classées et non classées , on page 443.

Mises à jour et rapports des ensembles de catégories d'URL

L'ensemble de catégories d'URL prédéfinies peut être mis à jour régulièrement et automatiquement sur votre Secure Web Appliance.

Lorsque ces mises à jour se produisent, les noms des anciennes catégories continueront d'apparaître dans les rapports jusqu'à ce que les données associées aux anciennes catégories soient trop anciennes pour être incluses dans les rapports. Les données de rapport générées après la mise à jour d'un ensemble de catégories d'URL utiliseront les nouvelles catégories. Vous pouvez donc voir les anciennes catégories et les nouvelles dans le même rapport.

Utilisation de la page URL Categories (Catégories d'URL) en association avec les pages Other Reporting (Autres rapports)

La page URL Categories (Catégories d'URL) peut être utilisée conjointement avec Page Application Visibility (Visibilité des applications), on page 434, Page User Details (Détails des utilisateurs) (Web Reporting [Création de rapports Web]) , on page 446 et Page Users (Utilisateurs), on page 445 pour enquêter sur un utilisateur en particulier et les types d'applications ou de sites Web auxquels un utilisateur tente d'accéder.

Par exemple, à partir de Page URL Categories (Catégories d'URL), on page 440, vous pouvez générer un rapport général pour les ressources humaines qui détaille toutes les catégories d'URL visitées par le site. À partir de la même page, vous pouvez obtenir des détails supplémentaires dans le tableau interactif URL Categories (Catégories d'URL) sur la catégorie d'URL « Streaming Media » (Diffusion multimédia en flux continu). En cliquant sur le lien de la catégorie Streaming Media (Diffusion multimédia en flux continu), vous pouvez afficher la page du rapport spécifique aux catégories d'URL. Cette page affiche non seulement les principaux utilisateurs qui visitent les sites de diffusion multimédia en flux continu (dans la section Top Users by Category for Total Transactions (Principaux utilisateurs par catégorie pour le total des transactions)), mais elle affiche également les domaines visités (dans le tableau interactif Domains Matched (Domaines correspondants)), comme YouTube.com ou QuickPlay.com.

À ce stade, vous obtenez de plus en plus d'informations précises concernant un utilisateur en particulier. Imaginons maintenant que cet utilisateur se distingue par son utilisation et que vous souhaitez savoir exactement à quelles informations il accède. De là, vous pouvez cliquer sur l'utilisateur dans le tableau interactif Users (Utilisateurs). Cette action vous amène au Page Users (Utilisateurs), on page 445, où vous pouvez afficher les tendances de la consommation pour cet utilisateur et découvrir exactement ce qu'il fait sur le Web.

Si vous souhaitez aller plus loin, vous pouvez maintenant accéder aux détails du suivi Web en cliquant sur le lien Transactions Completed (Transactions terminées) dans le tableau interactif. Cela affiche la section Recherche de transactions traitées par les services du proxy Web, on page 459 sur la page de suivi Web où vous pouvez voir les détails réels concernant les dates auxquelles l'utilisateur a accédé aux sites, l'URL complète, le temps passé sur cette URL, etc.

Signalisation des URL mal classées et non classées

Vous pouvez signaler les URL mal classées et non classées à l'adresse suivante :

https://talosintelligence.com/tickets.

Les soumissions sont évaluées en vue d'être incluses dans les mises à jour ultérieures des règles.

Pour vérifier l'état des URL envoyées, cliquez sur l'onglet **Status on Submitted URLs** (État des URL envoyées) sur cette page.

Page HTTPS Reports (Rapports HTTPS)

La page HTTPS Reports (Rapports HTTPS) est une agrégation globale du résumé du trafic HTTP/HTTPS (transactions ou utilisation de la bande passante) sur les appliances gérées.

Vous pouvez également afficher le résumé des chiffrements pris en charge en fonction des connexions côté client ou côté serveur, pour le trafic Web HTTP/HTTPS individuel qui traverse l'appliance gérée.

Pour afficher la page HTTPS Reports (Rapports HTTPS), sélectionnez **Monitoring > HTTPS Reports** (Supervision > Rapports HTTPS) dans la liste déroulante **Reports** (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Tableau 15 : Détails sur la page HTTPS Reports (Rapports HTTPS)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Modification de la plage de temps, à la page 401.

Section	Description
Web Traffic Summary (Résumé du trafic Web)	Vous pouvez afficher le résumé du trafic Web sur l'appliance de l'une des manières suivantes : • **Transactions** : sélectionnez cette option dans la liste déroulante pour afficher le résumé du trafic Web en fonction du nombre de transactions Web HTTP ou HTTPS, au format graphique, et le pourcentage de transactions Web HTTP ou HTTPS au format tabulaire. • **Bandwidth Usage** (Utilisation de la bande passante) : sélectionnez cette option dans la liste déroulante pour afficher le résumé du trafic Web en fonction de la quantité de bande passante utilisée par le trafic Web HTTP ou HTTPS, au format graphique, et le pourcentage d'utilisation de la bande passante HTTP ou HTTPS au format tabulaire.
Trend: Web Traffic (Tendance : trafic Web)	Vous pouvez afficher le graphique de tendance du trafic Web sur l'appliance en fonction de la plage de temps requise de l'une des manières suivantes : • **Web Traffic Trend** (Tendance du trafic Web) : sélectionnez cette option dans la liste déroulante pour afficher la tendance cumulative du trafic Web HTTP et HTTPS en fonction des transactions ou de l'utilisation de la bande passante. • **HTTPS Trend** (Tendance HTTPS) : sélectionnez cette option dans la liste déroulante pour afficher la tendance du trafic Web HTTPS en fonction des transactions ou de l'utilisation de la bande passante. • **HTTP Trend** (Tendance HTTP) sélectionnez cette option dans la liste déroulante pour afficher la tendance du trafic Web HTTP en fonction des transactions ou de l'utilisation de la bande passante.
Ciphers (Chiffrements)	Vous pouvez afficher le résumé des chiffrements de l'une des manières suivantes : • **By Client Side Connections** (Par connexions côté client) : sélectionnez cette option dans la liste déroulante pour afficher le résumé des chiffrements utilisés côté client du trafic Web HTTP ou HTTPS au format graphique. • **By Server Side Connections** (Par connexions côté serveur) : sélectionnez cette option dans la liste déroulante pour afficher le résumé des chiffrements utilisés côté serveur du trafic Web HTTP ou HTTPS au format graphique.

Page Users (Utilisateurs)

La page de rapport **Users** (Utilisateurs) fournit plusieurs liens qui vous permettent d'afficher les renseignements sur les rapports Web pour des utilisateurs individuels.

Pour afficher la page de rapport sur les utilisateurs, sélectionnez **Monitoring > Users** (Supervision > Utilisateurs) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Dans la page **Users** (Utilisateurs), vous pouvez voir combien de temps un utilisateur ou les utilisateurs de votre système ont passé sur Internet, sur une URL ou un site particulier, et la quantité de bande passante utilisée par cet utilisateur.

Remarque Le nombre maximal d'utilisateurs sur Secure Web Appliance que l'appliance de gestion de la sécurité peut prendre en charge est de 500.

Dans la page **Users** (Utilisateurs), vous pouvez afficher les informations suivantes concernant les utilisateurs de votre système :

Tableau 16 : Détails sur la page Users (Utilisateurs)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Top Users: Transactions Blocked (Principaux utilisateurs : Transactions bloquées)	Vous pouvez afficher les principaux utilisateurs, par adresse IP ou par nom d'utilisateur, et le nombre de transactions qui ont été bloquées, spécifiquement pour cet utilisateur, au format graphique. Le nom d'utilisateur ou l'adresse IP peut être anonymisé aux fins du rapport. Pour en savoir plus sur la façon d'anonymiser les noms d'utilisateurs dans cette page ou dans les rapports planifiés, consultez le *Guide de l'utilisateur d'AsyncOS pour les appliances Cisco Content Security Management*. Par défaut, tous les noms d'utilisateur s'affichent. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Top Users: Bandwidth Used (Principaux utilisateurs : Bande passante utilisée)	Vous pouvez afficher les principaux utilisateurs, par adresse IP ou par nom d'utilisateur, qui utilisent le plus de bande passante sur le système, au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.

Section	Description
Users (Utilisateurs)	Vous pouvez utiliser ce tableau interactif pour rechercher un ID utilisateur ou une adresse IP de client spécifique. Dans le champ de texte au bas du tableau User (Utilisateur), saisissez l'ID utilisateur ou l'adresse IP du client, puis cliquez sur Find User ID/Client IP Address (Rechercher un ID utilisateur ou une adresse IP du client). Il n'est pas nécessaire que l'adresse IP soit une correspondance exacte pour renvoyer des résultats. Vous pouvez cliquer sur un utilisateur en particulier pour obtenir des informations plus précises. Pour plus d'information, consultez Page User Details (Détails des utilisateurs) (Web Reporting [Création de rapports Web]) , à la page 446

Remarque Pour afficher les ID utilisateur plutôt que les adresses IP des clients, vous devez configurer votre appliance de gestion de la sécurité de façon à obtenir les renseignements sur l'utilisateur à partir d'un serveur LDAP.

Page User Details (Détails des utilisateurs) (Web Reporting [Création de rapports Web])

La page **User Details** (Détails sur l'utilisateur) vous permet d'afficher des informations spécifiques sur un utilisateur que vous avez identifié dans le tableau interactif de la page du rapport sur les utilisateurs.

La page User Details (Détails sur l'utilisateur) vous permet d'enquêter sur l'activité de chaque utilisateur sur votre système. Cette page est particulièrement utile si vous effectuez des enquêtes au niveau de l'utilisateur et que vous avez besoin de savoir, par exemple, quels sites vos utilisateurs visitent, à quelles menaces liées à des programmes malveillants ils sont confrontés, à quelles catégories d'URL ils accèdent et combien de temps un utilisateur spécifique passe sur ces sites.

Pour afficher la page User Details (Détails sur l'utilisateur) concernant un utilisateur en particulier, cliquez sur un utilisateur spécifique dans le tableau interactif Users (Utilisateurs) dans la page du rapport **Users** (Utilisateurs).

La page User Details (Détails sur l'utilisateur) vous permet d'afficher les renseignements suivants concernant un utilisateur individuel de votre système :

Tableau 17 : Détails sur la page User Details (Détails sur l'utilisateur)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.

Section	Description
URL Categories: Total Transactions (Catégories d'URL : transactions totales)	Vous pouvez afficher les catégories d'URL spécifiques utilisées par un utilisateur particulier au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. L'ensemble de catégories d'URL prédéfinies est mis à jour occasionnellement. Pour plus d'informations sur l'incidence de ces mises à jour sur les résultats des rapports, consultez Mises à jour et rapports des ensembles de catégories d'URL , à la page 416.
Trend: Total Transactions (Tendance : Transactions totales)	Vous pouvez utiliser ce graphique de tendance pour afficher toutes les transactions Web d'un utilisateur en particulier. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. Par exemple, ce graphique indique s'il y a un pic important du trafic Web à certaines heures de la journée et quand ces pics se produisent. À l'aide de la liste déroulante Time Range (Plage d'heures), vous pouvez développer ce graphique pour afficher une période de temps plus ou moins granulaire pendant laquelle cet utilisateur a consulté le Web.
URL Categories Matched (Catégories d'URL correspondantes)	Le tableau interactif correspondant aux catégories d'URL affiche les catégories correspondantes pour les transactions terminées et bloquées. Vous pouvez rechercher une catégorie d'URL spécifique dans le champ de texte au bas du tableau et cliquer sur **Find URL Category** (Rechercher une catégorie d'URL). Il n'est pas nécessaire que la catégorie soit exacte. L'ensemble de catégories d'URL prédéfinies est mis à jour occasionnellement. Pour plus d'informations sur l'incidence de ces mises à jour sur les résultats des rapports, consultez Mises à jour et rapports des ensembles de catégories d'URL , à la page 416.
Domains Matched (Domaines correspondants)	Le tableau interactif Domains Matched (Domaines correspondants) affiche les domaines ou les adresses IP auxquels l'utilisateur a accédé. Vous pouvez également afficher le temps passé sur ces catégories et diverses autres informations que vous avez définies dans la vue en colonne. Vous pouvez rechercher un domaine ou une adresse IP spécifique dans le champ de texte au bas du tableau et cliquer sur **Find Domain or IP** (Rechercher un domaine ou une adresse IP). Il n'est pas nécessaire que le domaine ou l'adresse IP soit exact.

Section	Description
Applications Matched (Applications correspondantes)	Le tableau interactif Applications Matched (Applications correspondantes) affiche les applications qu'un utilisateur spécifique utilise. Par exemple, si un utilisateur accède à un site qui nécessite l'utilisation de beaucoup de vidéos Flash, vous verrez le type d'application dans la colonne Application. Vous pouvez rechercher un nom d'application spécifique dans le champ de texte au bas du tableau et cliquer sur **Find Application** (Rechercher une application). Le nom de l'application n'a pas besoin d'être exact.
Cisco Secure Endpoint Threats Detected (Menaces détectées Cisco Secure Endpoint)	Le tableau interactif Cisco Secure Endpoint Threats Detected (Menaces détectées Cisco Secure Endpoint) affiche les fichiers de programmes malveillants détectés par le moteur Cisco Secure Endpoint. Vous pouvez rechercher des données sur une valeur SHA spécifique du fichier de programme malveillant, dans le champ de texte au bas du tableau et cliquer sur **Find malware Threat File SHA 256** (Rechercher les informations SHA 256 du fichier de programme malveillant). Le nom de l'application n'a pas besoin d'être exact.
Malware Threats Detected (Programmes malveillants détectés)	Le tableau interactif Malware Threats Detected (Programmes malveillants détectés) présente les principaux programmes malveillants déclenchés par un utilisateur spécifique. Vous pouvez rechercher des données sur un nom de programme malveillant spécifique dans le champ de texte au bas du tableau, puis cliquer sur **Find Malware Threat** (Rechercher un programme malveillant). Il n'est pas nécessaire que le nom du programme malveillant soit exact.
Policies Matched (Politiques correspondantes)	Le tableau interactif Policies Matched (Politiques correspondantes) affiche les groupes de politiques qui ont été appliqués à cet utilisateur lors de l'accès au Web. Vous pouvez rechercher un nom de politique spécifique dans le champ de texte au bas du tableau, puis cliquer sur **Find Policy** (Rechercher une politique). Le nom de la politique ne doit pas forcément être exact.

Remarque À partir du tableau des détails sur les risques liés aux programmes malveillants pour les clients : les rapports sur les clients affichent parfois un utilisateur avec un astérisque (*) à la fin du nom d'utilisateur. Par exemple, le rapport client peut afficher une entrée pour « jdupont » et « jdupont* ». Les noms d'utilisateur suivis d'un astérisque (*) sont ceux fournis par l'utilisateur, mais pas confirmés par le serveur d'authentification. Cela se produit lorsque le serveur d'authentification n'était pas disponible à ce moment-là et que l'appliance est configurée pour autoriser le trafic lorsque le service d'authentification n'est pas disponible.

Page Web Sites (Sites Web)

La page de rapport sur les **sites Web** est une agrégation globale de l'activité qui se produit sur les appliances gérées. Vous pouvez utiliser cette page de rapport pour surveiller les sites Web à haut risque consultés au cours d'une plage de temps spécifique.

Pour afficher la page de rapport sur les sites Web, sélectionnez **Monitoring > Web Sites** (Supervision >Sites Web) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

À partir de la page Web Sites (Sites Web), vous pouvez afficher les informations suivantes :

Tableau 18 : Détails sur la page Web Sites (Sites Web)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Top Domains: Total Transactions (Principaux domaines : total des transactions)	Vous pouvez afficher les principaux domaines visités sur le site Web au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Top Domains: Transactions Blocked (Principaux domaines : transactions bloquées)	Vous pouvez afficher les principaux domaines qui ont déclenché une action de blocage par transaction au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458. Par exemple, un utilisateur a accédé à un domaine particulier et, en raison d'une politique spécifique que j'ai en place, cela a déclenché une action de blocage. Ce domaine est répertorié dans ce graphique comme une transaction bloquée, et le site de domaine qui a déclenché l'action de blocage est répertorié.
Domains Matched (Domaines correspondants)	Vous pouvez utiliser ce tableau interactif pour rechercher les domaines qui sont visités sur le site Web. Vous pouvez cliquer sur un domaine spécifique pour accéder à des informations plus détaillées. L'onglet Proxy Services (Service de proxy) de la page de suivi Web s'affiche et vous pouvez voir les informations de suivi et savoir pourquoi certains domaines ont été bloqués. Lorsque vous cliquez sur un domaine spécifique, vous pouvez voir les principaux utilisateurs de ce domaine, les principales transactions sur ce domaine, les catégories d'URL correspondantes et les menaces liées à des programmes malveillants qui ont été détectées.

Page Cisco Secure Endpoint

Cisco Secure Endpoint offre une protection contre les menaces « jour zéro » et basées sur les fichiers en :

- obtenant la réputation des fichiers connus ;
- analysant le comportement de certains fichiers qui ne sont pas encore connus du service de réputation ;
- évaluant les menaces émergentes au fur et à mesure que de nouvelles informations sont disponibles et en vous informant au sujet des fichiers qui sont considérés comme des menaces après leur entrée dans votre réseau.

Pour plus d'informations sur le filtrage de réputation de fichiers et l'analyse de fichiers, consultez le guide de l'utilisateur ou l'aide en ligne d'*AsyncOS pour Secure Web Appliance*.

La page de rapport Cisco Secure Endpoint affiche les vues de rapport suivantes :

- Cisco Secure Endpoint - Page Summary (Résumé) Cisco Secure Endpoint
- Cisco Secure Endpoint - Page File Analysis (Analyse des fichiers)

Pour afficher la page de rapport Cisco Secure Endpoint, choisissez **Monitoring** (Supervision) > **Cisco Secure Endpoint** dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Cisco Secure Endpoint - Page Summary (Résumé) Cisco Secure Endpoint

La section Summary (Résumé) Cisco Secure Endpoint de la page de rapport Cisco Secure Endpoint affiche les menaces basées sur les fichiers qui ont été identifiées par le service File Reputation.

Pour voir les utilisateurs qui ont essayé d'accéder à chaque SHA et les noms de fichiers associés à ce SHA-256, cliquez sur un SHA-256 dans le tableau.

Vous pouvez cliquer sur le lien dans le tableau interactif des fichiers de programmes malveillants pour afficher toutes les instances du fichier dans le suivi Web qui ont été rencontrées dans la plage de temps maximale disponible, quelle que soit la plage sélectionnée pour le rapport.

Si un fichier extrait d'un fichier compressé ou archivé est malveillant, seule la valeur SHA du fichier compressé ou archivé est incluse dans le rapport Cisco Secure Endpoint.

Vous pouvez utiliser la section de résumé Cisco Secure Endpoint de la page Cisco Secure Endpoint pour afficher :

- Le résumé des fichiers identifiés par le service de réputation des fichiers du moteur Cisco Secure Endpoint, au format graphique.
- Les principaux fichiers de programmes malveillants au format graphique.
- Les principaux fichiers de menaces en fonction des types de fichiers au format graphique.
- Un graphique de tendance pour tous les fichiers de menaces par programmes malveillants selon la plage de temps sélectionnée.
- Le tableau interactif des fichiers de programmes malveillants qui répertorie les principaux fichiers de menaces par les programmes malveillants.

- Le tableau interactif des fichiers avec changement de verdict rétrospectif qui répertorie les fichiers traités par cette appliance pour lesquels le verdict a changé depuis le traitement de la transaction. Pour plus d'informations sur cette situation, consultez la documentation de votre Secure Web Appliance.

  Dans le cas de plusieurs modifications de verdicts pour un seul protocole SHA-256, ce rapport affiche uniquement le dernier verdict, et non l'historique des verdicts.

  Si plusieurs Secure Web Appliance ont des mises à jour de verdict différentes pour le même fichier, le résultat avec le dernier horodatage s'affiche.

  Vous pouvez cliquer sur un lien SHA-256 pour afficher les résultats du suivi Web pour toutes les transactions qui ont inclus ce SHA-256 dans la plage de temps maximale disponible, quelle que soit la plage sélectionnée pour le rapport.

Cisco Secure Endpoint - Page File Analysis (Analyse des fichiers)

La section d'analyse de fichier de la page du rapport Cisco Secure Endpoint affiche l'heure et le verdict (ou verdict provisoire) pour chaque fichier envoyé pour analyse. L'appliance vérifie les résultats de l'analyse toutes les 30 minutes.

Pour les déploiements avec une appliance Cisco Cisco Secure Endpoint Malware Analytics sur site : les fichiers qui figurent dans la liste des fichiers autorisés sur l'appliance Cisco Cisco Secure Endpoint Malware Analytics s'affichent comme « sains ». Pour en savoir plus sur l'inscription des utilisateurs autorisés, consultez l'aide en ligne de Cisco Secure Endpoint Malware Analytics.

Accédez aux résultats détaillés de l'analyse, notamment les caractéristiques et le niveau de menace de chaque fichier.

Vous pouvez également afficher des détails supplémentaires sur une SHA directement sur le serveur qui a effectué l'analyse en recherchant la SHA ou en cliquant sur le lien Cisco Cisco Secure Endpoint Malware Analytics au bas de la page des détails de l'analyse de fichier.

Si un fichier extrait d'un fichier compressé ou archivé est envoyé pour analyse, seule la valeur SHA du fichier extrait est incluse dans le rapport d'analyse des fichiers.

Vous pouvez utiliser la section d'analyse de fichier de la page de rapport Cisco Secure Endpoint pour afficher :

- Le nombre de fichiers chargés pour l'analyse de fichiers par le service d'analyse de fichier du moteur Cisco Secure Endpoint.
- Une liste des fichiers pour lesquels des demandes d'analyse de fichier ont été terminées.
- Une liste des fichiers pour lesquels des demandes d'analyse de fichier sont en attente.

Page Anti-Malware (Protection contre les programmes malveillants)

La page de rapport **Anti-Malware** (Protection contre les programmes malveillants) est une page de rapport relative à la sécurité qui reflète les résultats de l'analyse effectuée par les moteurs d'analyse activés (Webroot, Sophos, McAfee et/ou analyse adaptative).

Pour afficher la page de rapport sur la protection contre les programmes malveillants, choisissez **Monitoring > Anti-Malware** (Supervision > Protection contre les programmes malveillants) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Vous pouvez utiliser cette page pour identifier et surveiller les menaces de programmes malveillants sur le Web.

Remarque Pour afficher les données relatives aux programmes malveillants détectés par la supervision du trafic de la couche 4, consultez Page Layer 4 Traffic Monitor (Supervision du trafic de la couche 4), à la page 436

Dans la page Anti-Malware (Protection contre les programmes malveillants), vous pouvez afficher les informations suivantes :

Tableau 19 : Détails sur la page Anti-Malware (Protection contre les programmes malveillants)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Principales catégorie de programmes malveillants	Vous pouvez afficher les principales catégories de programmes malveillants détectés par un type de catégorie donné, au format graphique. Consultez Descriptions des catégories de programmes malveillants, à la page 454 pour plus d'informations sur les catégories de programmes malveillants valides. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.
Principaux programmes malveillants	Vous pouvez afficher les principaux programmes malveillants au format graphique. Pour personnaliser l'affichage du graphique, cliquez sur dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458.

Section	Description
Malware Categories (Catégorie de programmes malveillants)	Le tableau interactif Malware Categories (Catégories de programmes malveillants) affiche des informations détaillées sur des catégories de programmes malveillants particulières qui sont affichées dans le tableau Top Malware Categories (Principales catégories de programmes malveillants). Cliquez sur l'un des liens dans le tableau interactif Malware Categories (Catégories de programmes malveillants) pour afficher des détails plus précis sur les catégories de programmes malveillants et l'endroit où elles se trouvent sur le réseau. Exception : un lien Outbreak Heuristics (Heuristique des épidémies) dans le tableau vous permet d'afficher un graphique indiquant quand les transactions de cette catégorie se sont produites. Consultez Descriptions des catégories de programmes malveillants, à la page 454 pour plus d'informations sur les catégories de programmes malveillants valides.
Malware Threats (Programmes malveillants)	Le tableau interactif Malware Threats (Programmes malveillants) affiche des informations détaillées sur les programmes malveillants affichés dans la section Top Malware Threats (Principaux programmes malveillants). Les menaces libellées « Outbreak » (Épidémie) accompagnées d'un numéro sont des menaces identifiées par la fonctionnalité d'analyse adaptative indépendamment des autres moteurs d'analyse.

Page Malware Category Report (Rapports sur les catégories de programmes malveillants)

Étape 1 Choisissez **Reporting > Anti-Malware** (Rapports > Protection contre les programmes malveillants).

Étape 2 Dans le tableau interactif Malware Categories (Catégories de programmes malveillants), cliquez sur une catégorie dans la colonne Malware Category (Catégorie de programmes malveillants).

Page Rapport Malware Threat (Menaces des programmes malveillants)

La page Malware Threat Report (Rapport sur les menaces des programmes malveillants) montre les clients exposés à une menace particulière, affiche une liste des clients potentiellement infectés et des liens vers la page des détails concernant le client. Le graphique de tendance en haut du rapport affiche les transactions surveillées et bloquées en raison d'une menace pendant la plage de temps spécifiée. Le tableau en bas affiche le nombre réel de transactions surveillées et bloquées pour une menace au cours de la plage de temps spécifiée.

Pour afficher ce rapport, cliquez sur une catégorie dans la colonne Malware Category (Catégorie de programmes malveillants) de la page du rapport Anti-Malware (Antiprogrammes malveillants).

Pour en apprendre davantage, cliquez sur le lien **Support Portal Malware Details** (Détails des programmes malveillants du portail d'assistance) sous le tableau.

Descriptions des catégories de programmes malveillants

Secure Web Appliance peut bloquer les types de programmes malveillants suivants :

Type de maliciel	Description
Logiciels publicitaires	Les logiciels publicitaires englobent tous les exécutables logiciels et les modules d'extension qui dirigent les utilisateurs vers les produits à vendre. Certaines applications de logiciels publicitaires ont des processus distincts qui s'exécutent simultanément et se surveillent mutuellement, garantissant ainsi que les modifications sont permanentes. Certaines variantes se permettent de s'exécuter à chaque démarrage de l'ordinateur. Ces programmes peuvent également modifier les paramètres de sécurité, en empêchant les utilisateurs de modifier les options de recherche de leur navigateur, leur bureau et d'autres paramètres système.
Objet de l'assistant du navigateur	Un objet assistant de navigateur est un module d'extension de navigateur qui peut remplir diverses fonctions liées à la diffusion de publicités ou au détournement de paramètres d'utilisateur.
Supervision de système commercial	Un moniteur système commercial est un logiciel ayant les caractéristiques d'un moniteur système qui peut être obtenu avec une licence légitime par des moyens légaux.
Composeur automatique	Un composeur est un programme qui utilise votre modem ou un autre type d'accès Internet pour vous connecter à une ligne téléphonique ou à un site qui vous fait accumuler des frais d'interurbain pour lesquels vous n'avez pas donné votre consentement complet, significatif et éclairé.
Logiciel espion générique	Un logiciel espion est un type de programme malveillant installé sur les ordinateurs qui recueille de petits éléments d'information sur les utilisateurs à l'insu des utilisateurs.
Détournement d'identité	Un pirate modifie les paramètres système ou toute modification indésirable apportée au système d'un utilisateur peut le diriger vers un site Web ou exécuter un programme sans le consentement complet, significatif et éclairé de l'utilisateur.
Autres programmes malveillants	Cette catégorie est utilisée pour détecter tous les autres programmes malveillants et comportements suspects qui n'entrent pas exactement dans l'une des autres catégories définies.
Heuristique des épidémies	Cette catégorie représente les programmes malveillants détectés par l'analyse adaptative indépendamment des autres moteurs de protection contre les programmes malveillants.
URL d'hameçonnage	Une URL d'hameçonnage s'affiche dans la barre d'adresse du navigateur. Dans certains cas, elle implique l'utilisation de noms de domaine et ressemble à celle de domaines légitimes. L'hameçonnage est une forme de vol d'identité en ligne qui recourt à la fois à l'ingénierie sociale et à des subterfuges techniques pour dérober des données d'identité personnelles et des identifiants de comptes financiers.
API (applications potentiellement indésirables)	Application potentiellement indésirable. Un PUA est une application qui n'est pas malveillante, mais qui peut être considérée comme indésirable.

Type de maliciel	Description
Moniteur système	Un moniteur système englobe tout logiciel qui effectue l'une des actions suivantes : Enregistre ouvertement ou secrètement les processus du système et/ou les actions de l'utilisateur; Rend ces enregistrements disponibles pour la récupération et l'examen ultérieurement.
Outil de téléchargement de chevaux de Troie	Un logiciel de téléchargement de chevaux de Troie désigne un cheval de Troie qui, après son installation, communique avec un hôte ou un site distant et installe des paquets ou des sociétés affiliées à partir de l'hôte distant. Ces installations se produisent généralement à l'insu de l'utilisateur. De plus, les données utiles d'un tel logiciel de téléchargement peuvent varier d'une installation à l'autre, car il obtient les instructions de téléchargement de l'hôte ou du site distant.
Cheval de Troie	Un cheval de Troie est un programme destructeur qui se fait passer pour une application inoffensive. Contrairement aux virus, les chevaux de Troie ne se reproduisent pas.
Cheval de Troie pour hameçonnage	Un cheval de Troie pour hameçonnage peut rester sur un ordinateur infecté en attendant la visite d'une page Web spécifique ou peut analyser l'ordinateur infecté à la recherche de noms d'utilisateur et de mots de passe pour des sites bancaires, des sites d'enchères ou des sites de paiement en ligne.
Virus	Un virus est un programme ou un élément de code qui est chargé sur votre ordinateur à votre insu et qui s'exécute contre votre volonté.
Vers	Un ver est un programme ou un algorithme qui se reproduit sur un réseau informatique et qui effectue généralement des actions malveillantes.

Page relative aux risques des programmes malveillants du client

La page **Reporting > Client Malware Risk** (Rapports > Risques liés aux programmes malveillants pour les clients) est une page de rapport sur la sécurité qui peut être utilisée pour surveiller les activités à risque des programmes malveillants pour les clients. La page Client Malware Risk (Risques liés aux programmes malveillants pour les clients) répertorie également les adresses IP des clients impliqués dans les connexions fréquentes de programmes malveillants, comme identifiées par la supervision du trafic de la couche 4 (L4TM).

Tableau 20 : Détails sur la page sur les risques liés aux programmes malveillants pour les clients

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Web Proxy: Top Clients Monitored or Blocked (Proxy Web : principaux clients surveillés ou bloqués)	Ce tableau affiche les dix principaux utilisateurs qui ont rencontré un risque lié à des programmes malveillants.

Section	Description
L4 Traffic Monitor: Malware Connections Detected (Supervision du trafic de la couche 4 : connexions à des programmes malveillants détectées)	Ce tableau affiche les adresses IP des ordinateurs de votre entreprise qui se connectent le plus souvent aux sites de programmes malveillants.
Web Proxy: Client Malware Risk (Proxy Web : risque lié aux programmes malveillants pour les clients)	Le tableau interactif Proxy Web : risque lié aux programmes malveillants pour les clients affiche des informations détaillées sur des clients particuliers qui sont affichées dans la section Web Proxy: Top Clients by Malware Risk (Proxy Web : risque lié aux programmes malveillants pour les clients).
L4 Traffic Monitor: Clients by Malware Risk (Supervision du trafic de la couche 4 : clients par risque lié aux programmes malveillants)	Le tableau interactif L4 Traffic Monitor: Clients by Malware Risk (Supervision du trafic de la couche 4 : Clients par risque lié aux programmes malveillants) affiche les adresses IP des ordinateurs de votre organisation qui se connectent fréquemment aux sites malveillants.

Page Web Reputation Filters (Filtres de réputation Web)

Vous pouvez utiliser la page de rapport **Web Reputation Filters** (Filtres de réputation Web) pour afficher les résultats des filtres de réputation Web définis pour les transactions effectuées pendant une plage de temps spécifiée.

Pour afficher la page de rapport Web Reputation Filters (Filtres de réputation Web), choisissez **Monitoring > Web Reputation Filters** (Supervision > Filtres de réputation Web) dans la liste déroulante Reports (Rapports). Pour en savoir plus, consultez Utilisation des pages de rapport interactives sur la nouvelle interface Web, à la page 406.

Que sont les filtres de réputation Web?

Les filtres de réputation Web analysent le comportement d'un serveur Web et attribuent un score de réputation à une URL pour déterminer la probabilité qu'elle contienne des programmes malveillants basés sur l'URL. Ils contribuent à assurer une protection contre les programmes malveillants basés sur les URL qui menacent la confidentialité et les informations sensibles de l'entreprise. Secure Web Appliance utilise les scores de réputation d'URL pour identifier les activités suspectes et arrêter les attaques de programmes malveillants avant qu'elles ne se produisent. Vous pouvez utiliser les filtres de réputation Web avec les politiques d'accès et de déchiffrement.

Les filtres de réputation Web utilisent des données statistiques pour évaluer la fiabilité des domaines Internet et la réputation des URL. Des données telles que la durée d'enregistrement d'un domaine spécifique, l'endroit où un site Web est hébergé ou si un serveur Web utilise une adresse IP dynamique sont utilisées pour juger de la fiabilité d'une URL donnée.

Le calcul de la réputation Web associe une URL à des paramètres réseau pour déterminer la probabilité que des programmes malveillants soient présents. La probabilité agrégée de la présence de programmes malveillants est ensuite mappée sur un indice de réputation Web compris entre -10 et +10, +10 étant la valeur la moins susceptible de contenir des programmes malveillants.

Voici des exemples de paramètres :

- Données de catégorisation d'URL
- Présence d'un code téléchargeable
- Présence de contrats de licence d'utilisateur final (CLUF) longs et brouillés
- Volume global et variations de volume
- Renseignements sur le propriétaire du réseau
- Historique d'une URL
- Âge d'une URL
- Présence sur toutes les listes de blocage
- Présence sur toutes les listes d'autorisation
- Fautes de frappe d'URL de domaines populaires
- Informations sur le bureau d'enregistrement de domaine
- Informations sur l'adresse IP

Pour en savoir plus sur le filtrage de réputation Web, consultez la section « Filtrage des catégories d'URL personnalisées » dans le *Guide de l'utilisateur pour AsyncOS pour Secure Web Appliance*.

Dans la page Filtres de réputation Web, vous pouvez afficher les informations suivantes :

Tableau 21 : Détails sur la page des filtres de réputation Web

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport. Pour obtenir plus d'informations, reportez-vous à la section Choix d'une plage de temps pour les rapports, à la page 402.
Web Reputation Actions (Trend) [Actions de réputation Web (tendance)]	Vous pouvez afficher le nombre total d'actions de réputation de sites Web par rapport à l'heure spécifiée au format graphique. À partir de là, vous pouvez voir les tendances potentielles au fil du temps pour les actions de réputation Web.
Web Reputation Actions (Volume) [Actions de réputation Web (volume)]	Vous pouvez afficher le volume d'actions de réputation Web en pourcentages par transaction.
Types de menaces de réputation Web bloqués par WBRS	Vous pouvez consulter les types de menaces détectées dans les transactions qui ont été bloquées par le filtrage de réputation Web au format graphique. **Remarque** WBRS ne peut pas toujours identifier le type de menace.

Section	Description
Threat Types Detected in Other Transactions (Types de menaces détectés dans d'autres transactions)	Vous pouvez consulter le type de menaces trouvées dans les transactions qui n'ont pas été bloquées par le filtrage de réputation Web sous forme graphique. Pour personnaliser l'affichage du graphique, cliquez sur ✓ dans le graphique. Pour en savoir plus, consultez (Rapports Web uniquement) Choix des données à représenter au format graphique, à la page 458. Voici les raisons pour lesquelles ces menaces n'ont pas été bloquées : • Toutes les menaces n'ont pas un score qui atteint le seuil de blocage. Cependant, d'autres fonctionnalités de l'appliance peuvent détecter ces menaces. • Les politiques peuvent être configurées pour permettre la transmission de menaces. **Remarque** WBRS ne peut pas toujours identifier le type de menace.
Web Reputation Actions (Breakdown by Score) [Actions de réputation Web (répartition par score de réputation)]	Si l'analyse adaptative n'est pas activée, ce tableau interactif affiche les scores de réputation Web décomposés pour chaque action.
Threat Categories Matched (Catégories de menaces correspondantes)	Vous pouvez afficher les catégories de menaces correspondantes au format graphique.

Ajustement des paramètres de réputation Web

En fonction des résultats de votre rapport, vous pouvez ajuster les paramètres configurés de réputation Web, par exemple ajuster les scores de seuil ou activer ou désactiver l'analyse adaptative. Pour des informations spécifiques sur la configuration des paramètres de réputation Web, consultez le *Guide de l'utilisateur d'AsyncOS pour Cisco Secure Web Appliance*.

(Rapports Web uniquement) Choix des données à représenter au format graphique

Les graphiques par défaut de chaque page de rapport Web affichent les données couramment référencées, mais vous pouvez choisir d'afficher des données différentes à la place. Si une page contient plusieurs graphiques, vous pouvez modifier chaque graphique.

En général, les options du graphique sont les mêmes que les colonnes du tableau du rapport. Cependant, certaines colonnes ne peuvent pas être représentées au format graphique.

Les graphiques reflètent toutes les données disponibles dans une colonne de tableau, quel que soit le nombre d'éléments (lignes) que vous choisissez d'afficher dans le tableau associé.

Étape 1 Cliquez sur ✓ dans un tableau en particulier.

Étape 2 Choisissez les données requises à afficher. L'aperçu du tableau s'affiche en fonction des options sélectionnées.

Étape 3 Cliquez sur **Apply** (Appliquer).

Suivi Web sur la nouvelle interface Web

Vous pouvez utiliser la page **Web Tracking Search** (Recherche de suivi Web) pour rechercher et afficher des détails sur des transactions individuelles ou des schémas de transactions qui peuvent présenter des préoccupations. Selon les services utilisés par votre déploiement, recherchez dans les onglets pertinents :

- Recherche de transactions traitées par les services du proxy Web, à la page 459
- Recherche de transactions traitées par la supervision du trafic de la couche 4, à la page 464
- Recherche de transactions traitées par le serveur proxy SOCKS , à la page 464
- Utilisation des résultats de recherche de suivi Web , à la page 465
- Affichage des détails de la transaction pour les résultats de recherche de suivi Web , à la page 466

Pour en savoir plus sur la distinction entre le proxy Web et la supervision du trafic de la couche 4, consultez la section « Comprendre comment fonctionne Secure Web Appliance » du *Guide de l'utilisateur d'AsyncOS pour Cisco Secure Web Appliance*.

Recherche de transactions traitées par les services du proxy Web

Vous pouvez utiliser l'onglet **Proxy Services** (Services proxy) sur la page **Web Tracking Search** (Recherche de suivi Web) pour rechercher les données de suivi Web agrégées à partir de composants de sécurité individuels et de composants d'application de conditions d'utilisation acceptable. Ces données n'incluent pas les données de supervision du trafic de la couche 4 ni les transactions traitées par le proxy SOCKS.

Vous pourriez souhaiter l'utiliser pour aider les rôles suivants :

- **Responsable des ressources humaines ou juridique.** Exécute un rapport d'enquête pour un employé pendant une période donnée.

  Par exemple, vous pouvez utiliser l'onglet Proxy Services (Services proxy) pour récupérer des informations sur une URL spécifique à laquelle un utilisateur accède, l'heure à laquelle l'utilisateur a consulté cette URL, si cette URL est autorisée, etc.

- **Administrateur de la sécurité réseau.** Vérifie si le réseau de l'entreprise est exposé à des programmes malveillants provenant des téléphones intelligents des employés.

Vous pouvez afficher les résultats de la recherche pour les transactions enregistrées (notamment les transactions bloquées, surveillées, ayant fait l'objet d'un avertissement et terminées) au cours d'une période donnée. Vous pouvez également filtrer les résultats de données en utilisant plusieurs critères, tels que la catégorie d'URL, le programme malveillant et l'application.

Remarque Le proxy Web fournit uniquement des rapports sur les transactions qui comprennent une balise de décision ACL autre que « OTHER-NONE ».

Pour obtenir un exemple d'utilisation de l'onglet Proxy Services (Services proxy) avec d'autres pages de rapports Web, consultez le .

Étape 1 Sur l'appliance de gestion de la sécurité, choisissez **Web** dans la liste déroulante.

Étape 2 Utilisation de la page URL Categories (Catégories d'URL) en association avec les pages Other Reporting (Autres rapports), à la page 442 Choisissez **Tracking > Proxy Services** (Suivi > Services proxy).

Étape 3 Pour voir toutes les options de recherche et de filtrage, cliquez sur **Advanced** (Avancé).

Étape 4 Saisissez les critères de recherche :

Tableau 22 : Critères de recherche de suivi Web sur l'onglet Proxy Services (Services proxy)

Option	Description
Default Search Criteria (Critères de recherche par défaut)	
Time Range (Plage de temps)	Choisissez la plage de temps sur laquelle porte le rapport. Pour en savoir plus sur les plages de temps disponibles sur l'appliance de gestion de la sécurité, consultez Choix d'une plage de temps pour les rapports, à la page 402.
User/Client IPv4 or IPv6 (Utilisateur/Client IPv4 ou IPv6)	Vous pouvez également saisir un nom d'utilisateur d'authentification tel qu'il apparaît dans les rapports ou l'adresse IP du client que vous souhaitez suivre. Vous pouvez également saisir une plage d'adresses IP au format CIDR, par exemple 172.16.0.0/16. Si vous laissez ce champ vide, la recherche renvoie des résultats pour tous les utilisateurs.
Website (Site Web)	Saisissez éventuellement un site Web que vous souhaitez suivre. Lorsque vous laissez ce champ vide, la recherche renvoie des résultats pour tous les sites Web.
Transaction Type (Type de transaction)	Choisissez le type de transactions que vous souhaitez suivre, soit All Transactions (Toutes les transactions), Completed (Terminé), Blocked (Bloqué), Monitored (Surpervisé) ou Warned (Ayant fait l'objet d'un avertissement).
Advanced Search Criteria (Critères de recherche avancée)	
URL Category (Catégorie URL)	Pour filtrer par catégorie d'URL, sélectionnez **Filter by URL Category** (Filtrer par catégorie d'URL) et saisissez la première lettre d'une catégorie d'URL personnalisée ou prédéfinie en fonction de laquelle effectuer le filtrage. Choisissez la catégorie dans la liste qui apparaît. Toutes les transactions récentes qui correspondent au nom de la catégorie sont incluses, quel que soit le nom du moteur indiqué dans la liste déroulante.

Option	Description
Malware Threat (Programmes malveillants)	Pour filtrer les données par programme malveillant spécifique, sélectionnez **Filter by Malware Threat** (Filtrer par programme malveillant) et entrez le nom du programme malveillant selon lequel effectuer le filtrage. Pour filtrer les données par catégorie de programmes malveillants, sélectionnez **Filter by Malware Category** (Filtrer par catégorie de programmes malveillants) et choisissez une catégorie de programmes malveillants en fonction de laquelle effectuer le filtrage. Pour une description, consultez Descriptions des catégories de programmes malveillants, à la page 454.
Application	Pour filtrer par application, sélectionnez **Application** et choisissez une application en fonction de laquelle effectuer le filtrage. Pour filtrer les données par type d'application, sélectionnez **Application Type** (Type d'application) et choisissez un type d'application selon lequel effectuer le filtrage.
WBRS	Dans la section WBRS, vous pouvez filtrer les données par score de réputation Web et par menace particulière pour la réputation Web. • Pour filtrer les données par score de réputation Web, sélectionnez **Score range** (Plage de score de réputation), puis les valeurs supérieure et inférieure selon lesquelles effectuer le filtrage. Vous pouvez également filtrer les sites Web qui n'ont aucun score de réputation en sélectionnant **No Score** (Aucun score de réputation). • Pour filtrer les données par menace pour la réputation Web, sélectionnez **Filter by Reputation Threat** (Filtrer par menace pour la réputation) et saisissez une menace pour la réputation Web en fonction de laquelle effectuer le filtrage. Pour en savoir plus sur les scores WBRS, consultez le Guide de l'utilisateur IronPort AsyncOS pour le Web.
Threat Category (Catégorie de menace)	Pour filtrer les données par catégorie de menace spécifique, développez la section **Threat Catégorie** (Catégorie de menace) et sélectionnez les catégories de menaces souhaitées. Pour sélectionner toutes les catégories de menaces disponibles, cliquez sur **Select All** (Sélectionner tout).
Youtube Category (Catégorie YouTube)	Pour filtrer les données par catégorie YouTube spécifique, développez la section **Youtube Category** (Catégorie YouTube) et sélectionnez les catégories YouTube que vous souhaitez afficher. Pour sélectionner toutes les catégories YouTube disponibles, cliquez sur **Select All** (Sélectionner tout). Vous pouvez également filtrer les données par catégories actives et inactives.
Policy (Politique)	Pour filtrer les données par groupe de politiques, sélectionnez **Policy** (Politique) et entrez un nom de groupe de politiques selon lequel effectuer le filtrage. Assurez-vous d'avoir déclaré la politique à l'aide de Secure Web Appliance.

Option	Description
AnyConnect Secure Mobility	Pour filtrer les données par accès distant ou local, sélectionnez **User Location** (Emplacement de l'utilisateur) et choisissez un type d'accès. Pour inclure tous les types d'accès, sélectionnez **Disable Filter** (Désactiver le filtre). (Dans les versions précédentes, cette option était appelée « Sécurité des utilisateurs mobiles ».)
Cisco Secure Endpoint	Pour filtrer les menaces basées sur les fichiers identifiées par le service de réputation des fichiers, entrez un nom de fichier dans le champ **Filename** (Nom de fichier). Pour filtrer les fichiers à l'aide du hachage SHA-256, entrez une valeur pour SHA-256 dans le champ **File SHA-256** (Informations SHA-256 du fichier). Pour filtrer les fichiers en fonction du verdict du fichier, sélectionnez Cisco Secure Endpoint **File Verdict** (Verdict du fichier) et choisissez un type de verdict. Les types de verdicts de fichier disponibles sont **Clean** (Sain), **Malicious** (Malveillant), **Unknown** (Inconnu), **UnScannable** (Impossible à analyser) et **Low risk** (Faible risque). Le type de verdict **Malicious** Malveillant) comprend trois sous-catégories : • **Malware**(Programmes malveillants) : fichiers bloqués pour des raisons autres qu'une détection personnalisée ou un seuil personnalisé. • **Custom Detection** (Détection personnalisée) : pourcentage d'informations SHA du fichier sur la liste de blocage reçue de la console Cisco Secure Endpoint. • **Custom Threshold** (Seuil personnalisé) : fichiers bloqués en raison des paramètres de seuil lors de la configuration de Cisco Secure Endpoint .
User Request (Demande utilisateur)	Pour filtrer les données selon les transactions qui ont été réellement initiées par l'utilisateur, sélectionnez **Filter by Web User-Requested Transactions** (Filtrer par transactions demandées par l'utilisateur Web). **Remarque :** lorsque vous activez ce filtre, les résultats de la recherche incluent les transactions de type « meilleure estimation ».

Descriptions des catégories de programmes malveillants

Secure Web Appliance peut bloquer les types de programmes malveillants suivants :

Type de maliciel	Description
Logiciels publicitaires	Les logiciels publicitaires englobent tous les exécutables logiciels et les modules d'extension qui dirigent les utilisateurs vers les produits à vendre. Certaines applications de logiciels publicitaires ont des processus distincts qui s'exécutent simultanément et se surveillent mutuellement, garantissant ainsi que les modifications sont permanentes. Certaines variantes se permettent de s'exécuter à chaque démarrage de l'ordinateur. Ces programmes peuvent également modifier les paramètres de sécurité, en empêchant les utilisateurs de modifier les options de recherche de leur navigateur, leur bureau et d'autres paramètres système.

Type de maliciel	Description
Objet de l'assistant du navigateur	Un objet assistant de navigateur est un module d'extension de navigateur qui peut remplir diverses fonctions liées à la diffusion de publicités ou au détournement de paramètres d'utilisateur.
Supervision de système commercial	Un moniteur système commercial est un logiciel ayant les caractéristiques d'un moniteur système qui peut être obtenu avec une licence légitime par des moyens légaux.
Composeur automatique	Un composeur est un programme qui utilise votre modem ou un autre type d'accès Internet pour vous connecter à une ligne téléphonique ou à un site qui vous fait accumuler des frais d'interurbain pour lesquels vous n'avez pas donné votre consentement complet, significatif et éclairé.
Logiciel espion générique	Un logiciel espion est un type de programme malveillant installé sur les ordinateurs qui recueille de petits éléments d'information sur les utilisateurs à l'insu des utilisateurs.
Détournement d'identité	Un pirate modifie les paramètres système ou toute modification indésirable apportée au système d'un utilisateur peut le diriger vers un site Web ou exécuter un programme sans le consentement complet, significatif et éclairé de l'utilisateur.
Autres programmes malveillants	Cette catégorie est utilisée pour détecter tous les autres programmes malveillants et comportements suspects qui n'entrent pas exactement dans l'une des autres catégories définies.
Heuristique des épidémies	Cette catégorie représente les programmes malveillants détectés par l'analyse adaptative indépendamment des autres moteurs de protection contre les programmes malveillants.
URL d'hameçonnage	Une URL d'hameçonnage s'affiche dans la barre d'adresse du navigateur. Dans certains cas, elle implique l'utilisation de noms de domaine et ressemble à celle de domaines légitimes. L'hameçonnage est une forme de vol d'identité en ligne qui recourt à la fois à l'ingénierie sociale et à des subterfuges techniques pour dérober des données d'identité personnelles et des identifiants de comptes financiers.
API (applications potentiellement indésirables)	Application potentiellement indésirable. Un PUA est une application qui n'est pas malveillante, mais qui peut être considérée comme indésirable.
Moniteur système	Un moniteur système englobe tout logiciel qui effectue l'une des actions suivantes : Enregistre ouvertement ou secrètement les processus du système et/ou les actions de l'utilisateur; Rend ces enregistrements disponibles pour la récupération et l'examen ultérieurement.

Type de maliciel	Description
Outil de téléchargement de chevaux de Troie	Un logiciel de téléchargement de chevaux de Troie désigne un cheval de Troie qui, après son installation, communique avec un hôte ou un site distant et installe des paquets ou des sociétés affiliées à partir de l'hôte distant. Ces installations se produisent généralement à l'insu de l'utilisateur. De plus, les données utiles d'un tel logiciel de téléchargement peuvent varier d'une installation à l'autre, car il obtient les instructions de téléchargement de l'hôte ou du site distant.
Cheval de Troie	Un cheval de Troie est un programme destructeur qui se fait passer pour une application inoffensive. Contrairement aux virus, les chevaux de Troie ne se reproduisent pas.
Cheval de Troie pour hameçonnage	Un cheval de Troie pour hameçonnage peut rester sur un ordinateur infecté en attendant la visite d'une page Web spécifique ou peut analyser l'ordinateur infecté à la recherche de noms d'utilisateur et de mots de passe pour des sites bancaires, des sites d'enchères ou des sites de paiement en ligne.
Virus	Un virus est un programme ou un élément de code qui est chargé sur votre ordinateur à votre insu et qui s'exécute contre votre volonté.
Vers	Un ver est un programme ou un algorithme qui se reproduit sur un réseau informatique et qui effectue généralement des actions malveillantes.

Recherche de transactions traitées par la supervision du trafic de la couche 4

L'onglet Layer 4 Traffic Monitor (Supervision du trafic de la couche 4) de la page de **recherche de suivi Web** fournit des détails sur les connexions aux ports et aux sites de programmes malveillants. Vous pouvez rechercher des connexions vers des sites de programmes malveillants à l'aide des types d'informations suivants :

- Plage de temps
- Adresse IP de l'ordinateur qui a lancé la transaction (IPv4 ou IPv6)
- Domaine ou adresse IP du site Web de destination (IPv4 ou IPv6)
- Port
- Adresse IP associée à un ordinateur au sein de votre organisation
- Type de connexion

Pour afficher le nom d'hôte sur le site douteux ou sur le Secure Web Appliance qui a traité la transaction, cliquez sur le lien Display Details (Afficher les détails) dans l'en-tête de colonne Destination IP Address (Adresses IP de destination).

Pour en savoir plus sur l'utilisation de ces informations, consultez Page Layer 4 Traffic Monitor (Supervision du trafic de la couche 4), à la page 436.

Recherche de transactions traitées par le serveur proxy SOCKS

Vous pouvez rechercher des transactions qui répondent à divers critères, notamment des transactions bloquées ou terminées; l'adresse IP de l'ordinateur client qui a lancé la transaction; et le domaine de destination, l'adresse

IP ou le port de destination. Vous pouvez également filtrer les résultats par catégorie d'URL personnalisée, correspondance de politiques et emplacement de l'utilisateur (local ou distant). Les adresses IPv4 et IPv6 ne sont pas prises en charge.

Étape 1 Choisissez **Tracking > SOCKS Proxy** (Suivi > Proxy SOCKS).

Étape 2 Pour voir toutes les options de recherche et de filtrage, cliquez sur **Advanced** (Avancé).

Étape 3 Saisissez les critères de recherche.

Étape 4 Cliquez sur **Search** (Recherche).

Prochaine étape

Thèmes connexes

Page SOCKS Proxy (Serveur mandataire SOCKS), à la page 439

Utilisation des résultats de recherche de suivi Web

Affichage de plus de résultats de recherche de suivi Web

Étape 1 Assurez-vous d'examiner toutes les pages de résultats renvoyés.

Étape 2 Pour afficher plus de résultats par page que le nombre actuellement affiché, sélectionnez une option dans le menu **Items Displayed** (Éléments affichés).

Étape 3 Si plus de transactions correspondent à vos critères que le nombre maximal de transactions offert dans le menu Items Displayed (Éléments affichés), vous pouvez consulter l'ensemble des résultats en cliquant sur le lien de **Printable Download** (Télécharger document imprimable) pour obtenir un fichier CSV qui comprend toutes les transactions correspondantes.

Ce fichier CSV comprend l'ensemble complet des données brutes, à l'exclusion des détails des transactions connexes.

Interprétation des résultats de recherche de suivi Web

Par défaut, les résultats sont triés par horodatage, le plus récent en premier.

Les résultats de la recherche comprennent :

- L'heure à laquelle l'URL a été consultée.
- Le nombre de transactions connexes générées par la transaction initiée par l'utilisateur, telles que les images chargées, les scripts javascript exécutés et les sites secondaires consultés. Le nombre de transactions

connexes s'affiche sur chaque ligne, sous le lien Display All Details (Afficher tous les détails) dans l'en-tête de colonne.

- La disposition (le résultat de la transaction. Le cas échéant, indique la raison pour laquelle la transaction a été bloquée, surveillée ou un avertissement.)

Affichage des détails de la transaction pour les résultats de recherche de suivi Web

Pour afficher	Faire ceci
L'URL complète d'une URL tronquée dans la liste	Notez quel hôte Secure Web Appliance a traité la transaction, puis consultez le journal des accès de cette appliance.
Détails d'une transaction individuelle	Cliquez sur une URL dans la colonne Website (Site Web).
Détails de toutes les transactions	Cliquez sur le lien **Display All Details...** (Afficher tous les détails) dans l'en-tête de la colonne Website (Site Web).
Une liste contenant jusqu'à 500 transactions connexes	Le nombre de transactions associées apparaît entre parenthèses sous le lien « Afficher les détails » dans l'en-tête de colonne de la liste des résultats de recherche. Cliquer sur le lien **Associated Transactions** (Transactions associées) dans la vue Details (Détails) pour une transaction.

À propos du suivi Web et des mises à niveau

Les nouvelles fonctionnalités de suivi Web peuvent ne pas s'appliquer aux transactions effectuées avant la mise à niveau, car les données requises peuvent ne pas avoir été conservées pour ces transactions. Pour connaître les limites possibles liées aux données de suivi Web et aux mises à niveau, consultez les notes de mise à jour correspondant à votre version.

Planification et archivage de rapports Web sur la nouvelle interface Web

Cette section aborde les points suivants :

- Planification des rapports Web sur la nouvelle interface Web, à la page 466
- Archivage de rapports Web sur la nouvelle interface Web, à la page 468

Planification des rapports Web sur la nouvelle interface Web

Cette section aborde les points suivants :

- Ajout de rapports Web planifiés sur la nouvelle interface Web, à la page 467

• Modification des rapports Web planifiés sur la nouvelle interface Web, à la page 468
• Suppression des rapports Web planifiés sur la nouvelle interface Web, à la page 468

Vous pouvez planifier l'exécution de rapports sur une base quotidienne, hebdomadaire ou mensuelle. Les rapports planifiés peuvent être configurés pour inclure les données de la journée précédente, des sept jours précédents, du mois précédent, du jour civil précédent (jusqu'à 250), du mois civil précédent (jusqu'à 12). Vous pouvez également inclure des données pour un nombre de jours personnalisé (de 2 jours à 100 jours) ou un nombre de mois personnalisé (de 2 mois à 12 mois).

Quel que soit le moment où vous exécutez un rapport, les données de l'intervalle de temps précédent (heure, jour, semaine ou mois) sont renvoyées. Par exemple, si vous planifiez l'exécution d'un rapport quotidien à 1 h, le rapport contiendra les données de la veille, de minuit à minuit (de minuit à 23:59).

Vous pouvez définir autant de destinataires que vous le souhaitez pour les rapports, y compris aucun destinataire. Si vous ne spécifiez pas de destinataire pour le courriel, le système archivera tout de même les rapports. Si vous devez envoyer les rapports à un grand nombre d'adresses, vous pouvez créer une liste d'envoi plutôt que d'énumérer les destinataires individuellement.

Ajout de rapports Web planifiés sur la nouvelle interface Web

Étape 1 Choisissez **Monitoring > Schedule & Archive** (Supervision > Planification et archivage).

Étape 2 Dans l'onglet Scheduled/Archived (Planifié/Archivé), cliquez sur le bouton **+**.

Étape 3 Sélectionnez votre type de rapport dans le menu déroulant **Report Type** (Type de rapport).

Étape 4 Dans le champ **Report Name** (Titre du rapport), saisissez le titre de votre rapport.

Pour éviter de créer plusieurs rapports du même nom, nous vous recommandons d'utiliser un titre descriptif.

Étape 5 Choisissez la plage de temps du rapport dans le menu déroulant **Time Range to Include** (Plage de temps à inclure).

Étape 6 Choisissez le format du rapport généré.

Le format par défaut est PDF.

Étape 7 Dans la section Delivery Options (Options de remise), choisissez l'une des options suivantes :

En sélectionnant cette option, le rapport sera répertorié dans la page Archived Reports (Rapports archivés).

Remarque Il n'est pas possible d'archiver les rapports de synopsis par domaine.

- Pour archiver le rapport, sélectionnez **Only Archive** (Archiver uniquement).
- Pour archiver et envoyer le rapport par courriel, cliquez sur **Archive and Email to Recipients** (Archiver et envoyer par courriel aux destinataires).
- Pour envoyer le rapport par courriel, cliquez sur **Only Email to Recipients** (Envoyer par courriel seulement aux destinataires).

Dans le champ **Email IDs** (ID d'e-mail), saisissez les adresses de messagerie des destinataires.

Étape 8 Dans la zone **Schedule** (Planification), sélectionnez le bouton d'option à côté du jour, de la semaine ou du mois pour votre rapport planifié.

Étape 9 Sélectionnez la langue dans laquelle le rapport doit être généré dans la liste déroulante **Report Language** (Langue du rapport).

Étape 10 Cliquez sur **Submit** (Soumettre).

Modification des rapports Web planifiés sur la nouvelle interface Web

Pour modifier des rapports sur la nouvelle interface Web de votre appliance, choisissez la page **Monitoring > Scheduled & Archive** (Supervision > Rapports planifiés et archive). Cliquez sur le lien correspondant au titre du rapport que vous souhaitez modifier. Modifiez les paramètres, puis cliquez sur **Edit** (Modifier) pour envoyer vos modifications sur la page.

Suppression des rapports Web planifiés sur la nouvelle interface Web

Pour supprimer des rapports sur la nouvelle interface Web de votre appliance, choisissez la page **Monitoring > Scheduled / Archived** (Supervision > Planifié/Archivé). Cochez les cases correspondant aux rapports que vous souhaitez supprimer et cliquez sur l'icône de la corbeille.

Pour supprimer tous les rapports planifiés, cochez la case à côté du titre du rapport. Notez que les versions archivées des rapports supprimés ne sont pas supprimées.

Archivage de rapports Web sur la nouvelle interface Web

[Nouvelle interface Web] Génération de rapports Web à la demande

Vous pouvez également générer à la demande la plupart des rapports que vous pouvez planifier.

Pour générer un rapport sur demande, procédez comme suit :

Étape 1 Dans Secure Web Appliance, choisissez **Monitoring > Schedule & Archive** (Supervision > Planification et archivage).

Étape 2 Dans l'onglet **View Archived** (Afficher l'archive), cliquez sur le bouton +.

Étape 3 Dans la section **Report Type** (Type de rapport), choisissez un type de rapport dans la liste déroulante.

Les options de la page peuvent changer.

Étape 4 Dans la section **Report Name** (Titre du rapport), saisissez le titre du rapport.

AsyncOS ne vérifie pas le caractère unique des noms de rapport. Pour éviter toute erreur, ne créez pas plusieurs rapports portant le même nom.

Étape 5 Dans la liste déroulante **Time Range to Include** (Plage de temps à inclure), sélectionnez une plage de temps pour les données du rapport.

Étape 6 Dans la section **Attachment Details** (Détails des pièces jointes), choisissez le format du rapport.

PDF. Créez un document PDF mis en forme pour la remise, l'archivage ou les deux. Vous pouvez consulter immédiatement le rapport au format PDF en cliquant sur Preview PDF Report (Survol du rapport PDF).

Étape 7 Dans la section **Delivery Options** (Options de remise), choisissez l'une des options suivantes :

En sélectionnant cette option, le rapport sera répertorié dans la page Archived Reports (Rapports archivés).

Remarque Il n'est pas possible d'archiver les rapports de synopsis par domaine.

- Pour archiver le rapport, sélectionnez **Only to Archive** (Archiver uniquement).
- Pour archiver et envoyer le rapport par courriel, cliquez sur **Archive and Email to Recipients** (Archiver et envoyer par courriel aux destinataires).
- Pour envoyer le rapport par courriel, cliquez sur **Only Email to Recipients** (Envoyer par courriel seulement aux destinataires).

Dans le champ **Email IDs** (ID d'e-mail), saisissez les adresses de messagerie des destinataires.

Étape 8 Sélectionnez la langue dans laquelle le rapport doit être généré dans la liste déroulante **Report Language** (Langue du rapport).

Étape 9 Cliquez sur **Deliver This Report** (Remettre ce rapport) pour générer le rapport.

Affichage et gestion des rapports Web archivés sur la nouvelle interface Web

Utilisez les renseignements de cette section pour utiliser les rapports générés en tant que rapports planifiés.

Étape 1 Connectez-vous à la nouvelle interface Web de votre appliance.

Étape 2 Sélectionnez **Monitoring > Schedule& Archive** (Supervision > Planifier et archiver).

Étape 3 Sélectionnez l'onglet **View Archived** (Afficher l'archive).

Étape 4 Pour afficher un rapport, cliquez sur le nom du rapport dans la colonne **Report Title** (Titre du rapport). La liste déroulante Report Type (Type de rapport) filtre les types de rapports répertoriés sous l'onglet **Archived Reports** (Rapports archivés).

Étape 5 Vous pouvez rechercher un rapport en particulier dans la zone de recherche.

Page System Status (État du système) sur la nouvelle interface Web

Dans l'écran Secure Web Appliance, choisissez **Monitoring > System Status** (Supervision > État du système) pour surveiller l'état du système. Cette page affiche l'état et la configuration actuels de Secure Web Appliance. L'heure du navigateur est affichée sur la page d'état du système dans le coin supérieur droit.

La page **System Status** (État du système) affiche les onglets suivants :

- Capacité

L'onglet **Status** (État) s'affiche par défaut.

État

La page d'état affiche les informations suivantes :

Cette section...	Description
État Secure Web Appliance	• Disponibilité du système • Utilisation des ressources système : utilisation du processeur, de la RAM et pourcentage d'espace disque utilisé pour les rapports et la journalisation. L'utilisation de la RAM pour un système qui fonctionne efficacement peut être supérieure à 90 %, car la RAM qui n'est pas autrement utilisée par le système est utilisée par le cache d'objets Web. Si votre système ne connaît pas de problèmes de performances graves et que cette valeur n'est pas bloquée à 100 %, le système fonctionne normalement. **Remarque** La mémoire tampon du proxy est un composant qui utilise cette RAM.
Alerts (Alertes)	Affiche le nom des alertes, ainsi que la date et l'heure auxquelles l'alerte s'est produite. Lorsque vous cliquez sur **More** (Plus) dans le coin supérieur droit ou sur le nom d'une alerte, la fenêtre contextuelle **All Alerts** (Toutes les alertes) s'affiche. La ligne d'alerte sélectionnée est mise en surbrillance dans la fenêtre contextuelle **All Alerts** (Toutes les alertes). La fenêtre contextuelle **All Alerts** (Toutes les alertes) s'affiche : • Date et heure de l'alerte • Niveau d'alerte : Info, Avertissement ou Critique • Classe d'alerte • Problème – Description courte de l'alerte • Destinataire : adresse de messagerie à laquelle les détails de l'alerte sont envoyés
Disk Usage (Utilisation du disque)	Affiche la valeur d'utilisation du disque et l'état de stockage RAID. L'état du stockage RAID dépend de la configuration de l'appliance. Pour les appliances virtuelles, l'état de stockage RAID affiche « Unknown » (Inconnu) et pour les appliances physiques, il affiche « Optimal ».
Proxy Status (État du proxy)	Affiche l'utilisation du processeur du proxy et l'utilisation des E/S du disque proxy. Affiche également les connexions proxy en attente avec le numéro de port et le nombre de connexions.
High Availability (Haute disponibilité)	Affiche le nom, la priorité et l'état du groupe de basculement. Affiche également le nombre de groupes de basculement à haute disponibilité activés. S'il n'y a aucun groupe de basculement, l'état du service affiche « Not Configured ».

Cette section...	Description

Proxy Traffic Characteristics (Caractéristiques du trafic du proxy)	Affiche les caractéristiques de trafic de proxy suivantes :
	• Demandes par seconde
	• Bande passante
	• Temps de réponse
	• Ratio de résultats du cache
	• Connexions actuelles : nombre de connexions pour une heure et une date particulières, et affiche des détails comme les suivants :
	  • Connexions client inactives
	  • Connexions du serveur inactif
	  • Nombre total de connexions client
	  • Nombre total de connexions serveur
	
	Affiche les valeurs moyenne et maximale de ces données. Les valeurs moyennes sont affichées pour la dernière minute, la dernière heure et depuis le redémarrage du proxy. Les valeurs maximales sont affichées pour la dernière heure et depuis le redémarrage du proxy.
	Remarque Cliquez sur l'icône de lien à côté de RPS et de bande passante, qui vous redirige à l'onglet Capacité. De même, cliquez sur l'icône de lien à côté du temps de réponse, qui vous redirige à l'onglet Services.

Capacité

La page Capacity (Capacité) affiche les informations suivantes :

Cette section...	Description
Time Range (Plage de temps)	Affiche les options de plage de temps suivantes : • Hour (Heure) • Day (Jour) • Week (Semaine) • 30 Days (30 jours) • 90 Days (90 jours) • Yesterday (Hier) (00:00 à 23:59) • Previous Calendar Month (Mois calendaire précédent) • Custom Range (Plage personnalisée) : premières données disponibles Cliquez sur **Apply** (Appliquer) pour afficher les premières données disponibles, puis cliquez sur **Cancel** (Annuler) pour annuler l'opération. **Remarque** L'option Time Range (Plage de temps) s'applique à toutes les fonctionnalités de l'onglet Capacity (Capacité).
Utilisation du processeur système et de la mémoire	L'utilisation du processeur système et de la mémoire système vous permet d'effectuer les tâches suivantes : • Mettez à jour ou définissez la valeur de seuil (par exemple, 0 à 100 %). • Modifiez la valeur du seuil. • Affichez l'utilisation du processeur et de la mémoire. Les codes de couleur sont les suivants : • Rouge : indique la valeur du seuil. • Vert : indique la valeur moyenne. Si vous modifiez la valeur de seuil, la valeur moyenne est également mise à jour en conséquence. La valeur moyenne est la valeur de la somme divisée par la longueur des enregistrements. • Bleu : indique l'utilisation de la mémoire système en pourcentage. Les données d'utilisation de la mémoire et du processeur du système sont affichées en pourcentage en fonction de la plage de temps sélectionnée. Les données et le graphique changent de manière dynamique en fonction des données actuelles.
Bande passante et RPS	Affiche les détails suivants sur la bande passante et le système d'alimentation redondante sous forme graphique : • Général : Affiché en bleu marine • HTTPS déchiffré : s'affiche en bleu marine Cliquez sur les blocs de légende pour activer ou désactiver les informations globales et HTTPS déchiffrées.

Cette section...	Description
CPU Usage by Function (Utilisation du processeur par fonction)	Les codes de couleur pour les diverses options d'utilisation du processeur sont les suivants : • Vert clair : proxy Web • Vert Foncé : Journalisation • Mauve : rapports • Jaune : WBRS • Bleu foncé : Cisco Secure Endpoint • Bleu clair : Webroot • Bleu eau : Sophos • Gris : McAfee Cliquez sur les blocs de légende pour activer ou désactiver les options.
Client or Server Connection (Connexion du client ou du serveur)	Affiche les connexions moyenne et maximale et vous permet d'effectuer les tâches suivantes : • Activer ou désactiver la connexion moyenne et maximale • Afficher les détails et les graphiques de la connexion moyenne et maximale

Services

La page Services affiche les services et leur état. Le ruban des services affiche l'état des services Cisco Secure Endpoint , WCCP, ISE et CTR. La couleur à côté du nom du service indique son état :

- Rouge : le service n'est pas prêt.
- Gris : le service est prêt, mais désactivé.
- Vert : le service est prêt, activé et en cours d'exécution.

Cette section...	Description
Date	Les données de service pour la journée en cours sont affichées par défaut. Vous pouvez afficher les données des sept jours précédents. Choisissez une date dans le calendrier pour afficher les données du jour en particulier.

Cette section...	Description
Service Status (État du service)	Le tableau Service Status (État du service) affiche les événements et les alertes relatifs aux services. Le tableau affiche un intervalle de 24 heures, qui est divisé en plages d'une heure. Chaque bloc représente les alertes dans un intervalle de temps d'une heure. La couleur verte d'un bloc indique qu'il n'y a aucune alerte critique au cours de l'heure correspondante. S'il y a au moins une alerte critique par heure, le bloc correspondant s'affiche en rouge. Les blocs correspondant aux futures plages de temps sont affichés en blanc. L'icône sur le côté gauche près du nom du service affiche la couleur du dernier bloc (ou de l'heure en cours). Vous pouvez cliquer sur le bloc rouge pour voir les heures auxquelles les 5 dernières alertes se sont produites. Elle affiche également le nombre total d'alertes sous la forme *5 sur « n » événements*, « *n* » étant le nombre total d'alertes survenues au cours de cette période. Cliquez sur **More** (Plus) pour afficher la fenêtre contextuelle **All Alerts** (Toutes les alertes). La fenêtre contextuelle **All Alerts** (Toutes les alertes) s'affiche : • Date et heure de l'alerte • Niveau d'alerte : Info, Avertissement ou Critique • Classe d'alerte • Problème – Description courte de l'alerte • Destinataire : adresse de messagerie à laquelle les détails de l'alerte sont envoyés

Cette section...	Description
Service Response Time (Temps de réponse du service)	Le tableau Service Response Time (Temps de réponse du service) présente le modèle de temps de réponse de chaque service en cours d'exécution dans le système. Les heures suivantes sont affichées : • Durée du service McAfee • Durée du service WBRS • Temps de réponse DNS • Heure du service Webroot • Durée du service Cisco Secure Endpoint • Durée du service Sophos • Temps de réponse du serveur Le tableau affiche un intervalle de 24 heures divisé en plages de 1 heure. Chaque bloc représente le modèle de réponse du service dans une heure. Le temps de réponse de chaque service est fractionné dans les plages horaires suivantes : • 0,001 s à 0,06 s • 0,06 s à 0,6 s • 0,6 s à 1 s • 1 s à 6 s • 6 s et plus Par défaut, le tableau affiche les valeurs de réponse de 1 s à 6 s pour tous les services. Vous pouvez développer et afficher la scission détaillée. Le système calcule le temps de réponse pour toutes les transactions. Il affiche ensuite le pourcentage du volume de transactions qui a eu lieu dans chaque plage de temps. La couleur du bloc dépend du pourcentage du volume de transaction.

Cette section...	Description
	Pour les temps de réponse inférieurs à 1 seconde, la légende du volume de transactions est : • Bleu Foncé : 41 % à 100 % • Bleu eau : 11 % à 40 % • Bleu clair : 1 % à 10 % • Blanc : 0 % Pour un temps de réponse de 1 seconde et plus, la légende du volume de transaction est : • Rouge : 41 % à 100 % • Rouge clair : 26 % à 40 % • Bleu clair : 1 % à 25 % • Blanc : 0 % Lorsque les données pour le temps de réponse ne sont pas disponibles en secondes, l'option de couleur de légende est blanche et ne peut pas être modifiée. Cliquez sur l'option de plage de temps pour récupérer les données sur le temps de réponse du service. Les données comprennent les graphiques à barres et le nombre d'occurrences. Cependant, vous ne pouvez pas récupérer : • Graphique à barres • Données de légende pour les dates précédentes Cliquez sur une plage de temps pour ouvrir une fenêtre contextuelle qui affiche la tendance de la réponse dans un graphique à barres pour cette heure particulière. • Axe horizontal : plage horaire divisée en intervalles de 5 minutes • Axes vertical : nombre de transactions dans la plage de temps Passez la curseur sur un bloc de la fenêtre contextuelle pour voir le nombre de transactions dans cet intervalle de temps.

CHAPITRE 21

Détection du trafic non autorisé sur les ports non standard

Cette rubrique contient les sections suivantes :

Survol de la détection du trafic non autorisé

Secure Web Appliance intègre une supervision du trafic de la couche 4 qui détecte le trafic non autorisé sur tous les ports du réseau et arrête les tentatives de contournement du port 80 par les programmes malveillants. Lorsque des clients internes sont infectés par des programmes malveillants et tentent de téléphoner par le biais de ports et de protocoles non standard, la supervision du trafic de la couche 4 empêche l'activité de téléphone domestique de sortir du réseau de l'entreprise. Par défaut, la supervision du trafic de la couche 4 est activée et configurée pour surveiller le trafic sur tous les ports. Cela inclut le DNS et d'autres services.

La supervision du trafic de la couche 4 utilise et gère sa propre base de données interne. Cette base de données est continuellement mise à jour avec les résultats correspondants pour les adresses IP et les noms de domaine.

Configuration de la supervision du trafic de la couche 4

Étape 1 Configurez la supervision du trafic de la couche 4 à l'intérieur du pare-feu.

Étape 2 Assurez-vous que la supervision du trafic de la couche 4 est connectée « logiquement » après les ports proxy et avant tout périphérique qui effectue la traduction d'adresses réseau (NAT) sur les adresses IP des clients.

Étape 3 Configurer les paramètres globaux

Consultez Configuration des paramètres globaux de la supervision du trafic de la couche 4, on page 478.

Étape 4 Politiques de supervision du trafic de la couche 4

Consultez Création d'une politique pour détecter le trafic non autorisé, on page 479.

Liste des sites connus

Address (Adresse)	Description
Autorisé connu	Toute adresse IP ou tout nom d'hôte répertorié dans la propriété Allow List (Liste des adresses autorisées). Ces adresses apparaissent dans les fichiers journaux en tant qu'adresses de la « liste des adresses autorisées ».
Non publiée	Toute adresse IP qui n'est pas connue pour être un site malveillant ou qui n'est pas une adresse autorisée. Elle n'est pas répertoriée dans les propriétés de la liste des autorisations, des adresses supplémentaires de programmes malveillants suspects ou dans la base de données de la supervision du trafic de la couche 4. Ces adresses ne figurent pas dans les fichiers journaux.
Douteuse	Celles-ci apparaissent dans les fichiers journaux en tant qu'adresses de la « liste grise » et comprennent : • Toute *adresse IP* qui est associée à un *nom d'hôte* non publié et à un *nom d'hôte* connu d'un programme malveillant. • Toute *adresse IP* associée à un *nom d'hôte* non publié et à un *nom d'hôte* dans la propriété Additional Suspected Malware Addresses (Adresses supplémentaires suspectées de programme malveillant)
Programme malveillant connu	Celles-ci apparaissent dans les fichiers journaux en tant qu'adresses de « liste bloquée » et comprennent : • Toute adresse IP ou nom d'hôte que la base de données de la supervision du trafic de la couche 4 détermine comme étant un site malveillant connu et *non* répertorié dans la liste des adresses autorisées. • Toute *adresse IP* qui est répertoriée dans la propriété Additional Suspected Malware Addresses (Adresses supplémentaires pour les programmes malveillants suspects), qui *ne figure pas* dans la liste des autorisations et qui *n'est pas* douteuse.

Configuration des paramètres globaux de la supervision du trafic de la couche 4

Étape 1 Choisissez **Security Services > L4 Traffic Monitor** (Services de sécurité > Supervision du trafic de la couche 4).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Choisissez d'activer ou non la supervision du trafic de la couche 4.

Étape 4 Lorsque vous activez la supervision du trafic de la couche 4, choisissez les ports à surveiller :

- **All ports** (Tous les ports). Surveille tous les ports TCP 65535 pour détecter les activités non autorisées.

- **All ports except proxy ports** (Tous les ports, à l'exception des ports du proxy). Surveille tous les ports TCP, à l'exception des ports suivants, pour détecter les activités non autorisées.
  - Ports configurés dans la propriété « HTTP Ports to Proxy » (Ports HTTP vers proxy) sur la page Security Services > Web Proxy (Services de sécurité > Proxy Web) (généralement le port 80).
  - Ports configurés dans la propriété « Transparent HTTPS Ports to Proxy » (Ports HTTPS transparents vers proxy) dans la page Security Services > HTTPS Proxy (Services de sécurité > Proxy HTTPS) (généralement le port 443).

Étape 5 Envoyez et validez les modifications.

Mise à jour des règles de protection contre les programmes malveillants de la supervision du trafic de la couche 4

Étape 1 Choisissez **Security Services > L4 Traffic Monitor** (Services de sécurité > Supervision du trafic de la couche 4).

Étape 2 Cliquez sur **Update Now** (Mettre à jour maintenant).

Création d'une politique pour détecter le trafic non autorisé

Les actions effectuées par la supervision du trafic de la couche 4 dépendent des politiques de supervision du trafic de la couche 4 que vous configurez :

Étape 1 Choisissez **Web Security Manager > L4 Traffic Monitor** (Web Security Manager > Supervision du trafic de la couche 4).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la page **Edit L4 Traffic Monitor Policies** (Modifier les politiques de supervision du trafic de la couche 4), configurez les politiques de supervision du trafic de la couche 4 :

a) **Définir** la **liste des autorisations**

b) Ajouter des sites efficaces connus à la **liste des autorisations**

Note N'incluez pas le nom d'hôte ou l'adresse IP Secure Web Appliance dans la liste des autorisations, sinon la supervision du trafic de la couche 4 ne bloque aucun trafic.

c) Déterminez l'action à effectuer pour les **adresses de programmes malveillants suspects** :

Action	Description
Allow (Autoriser)	Autorise toujours le trafic vers et à partir d'adresses autorisées et non répertoriées connues

Action	Description
Monitor (Superviser)	Surpervise le trafic dans les circonstances suivantes : • Lorsque l'option Action for Suspected Malware Addresses (Action pour les adresses de programmes malveillants) est réglée sur Monitor (Superviser), elle surveille toujours tout le trafic qui ne va pas vers ou en provenance d'une adresse autorisée connue. • Lorsque l'option Action for Suspected Malware Addresses (Action en cas d'adresses malveillantes présumées) est définie sur Block (Bloquer), surveille le trafic à destination et en provenance des adresses douteuses.
Block (Bloquer)	Lorsque l'option Action for Suspected Malware Addresses (Action en cas d'adresses malveillantes présumées) est réglée sur Block (Bloquer), bloque le trafic à destination et en provenance d'adresses malveillantes connues.

Note – Lorsque vous choisissez de bloquer le trafic de programmes malveillants présumés, vous pouvez également choisir de toujours bloquer ou non les adresses douteuses. Par défaut, les adresses douteuses sont surveillées.

– Si la supervision du trafic de la couche 4 est configurée pour bloquer, la supervision du trafic de la couche 4 et le proxy Web doivent être configurés sur le même réseau. Utilisez la page **Network > Routes** (Réseau > Voies de routage) pour confirmer que tous les clients sont accessibles sur les voies de routage configurées pour le trafic de données.

- Dans une configuration VM, les demandes en mode transparent sont dupliquées en transitant par les interfaces P1 et T1 avec un décalage horaire intermittent. Par conséquent, certaines adresses IP, même après avoir été bloquées, peuvent transiter par l'appliance.

d) Définir les propriétés **Additional Suspected Malware Addresses** (Autres adresses malveillantes présumées)

Note L'ajout d'adresses IP internes à la liste d'adresses supplémentaires pour les programmes malveillants suspects fait que les URL de destination légitimes s'affichent comme des programmes malveillants dans les rapports de supervision du trafic de la couche 4. Pour éviter cela, n'entrez pas d'adresses IP internes dans le champ « **Additional Suspected Malware Addresses** » (Autres adresses malveillantes présumées) de la page **Web Security Manager > L4 Traffic Monitor Policies** (Web Security Manager > Politiques de supervision du trafic de la couche 4).

Étape 4 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Survol de la détection du trafic non autorisé, on page 477
- Formats valides, on page 481.

Formats valides

Lorsque vous ajoutez des adresses à la liste d'autorisation ou aux propriétés d'adresses supplémentaires pour les programmes malveillants suspects, séparez les entrées par des espaces ou des virgules. Vous pouvez saisir des adresses dans l'un des formats suivants :

- **Adresse IP IPv4.** Exemple : Format IPv4 : 10.1.1.0. Format IPv6 : 2002:4559:1FE2::4559:1FE2
- **Adresse CIDR** Exemple : 10.1.1.0/24.
- **Nom de domaine.** Exemple : exemple.com.
- **Nom d'hôte.** Exemple : crm.exemple.com.

Affichage de l'activité de la supervision du trafic de la couche 4

L'appliance S Series prend en charge plusieurs options pour générer des rapports spécifiques aux fonctionnalités et des affichages interactifs de statistiques sommaires.

Activité de supervision et affichage des statistiques sommaires

La page **Reporting > L4 Traffic Monitor** (Rapports > Supervision du trafic de la couche 4) fournit des résumés statistiques de l'activité de supervision. Vous pouvez utiliser les affichages et outils de création de rapports suivants pour afficher les résultats de l'activité de la supervision du trafic de la couche 4 :

Pour afficher...	Voir...
Statistiques relatives aux clients	Reporting > Client Activity (Rapports > Activité des clients)
Statistiques sur les programmes malveillants Statistiques relatives aux ports	Reporting > L4 Traffic Monitor (Rapports > Supervision du trafic de la couche 4)
Fichiers journaux de supervision du trafic de la couche 4	System Administration > Log Subscriptions (Administration système > Abonnements au journal) • trafmon_errlogs • trafmonlogs

Note Si le proxy Web est configuré comme proxy de transfert et que la supervision du trafic de la couche 4 est configurée pour surveiller tous les ports, l'adresse IP du port de données du proxy est enregistrée et affichée en tant qu'adresse IP client dans le rapport d'activité du client dans la page **Reporting > Client Activity** (Rapports > Activité du client). Si le proxy Web est configuré comme un proxy transparent, activez l'usurpation d'adresses IP pour enregistrer et afficher correctement les adresses IP des clients.

Entrées du fichier journal de supervision du trafic de la couche 4

Le fichier journal de supervision du trafic de la couche 4 fournit un enregistrement détaillé de l'activité de supervision.

CHAPITRE 22

Superviser l'activité du système au moyen de journaux

Cette rubrique contient les sections suivantes :

Survol de la journalisation

Le Secure Web Appliance enregistre ses propres activités de gestion du système et du trafic en les écrivant dans des fichiers journaux. Les administrateurs peuvent consulter ces fichiers journaux pour surveiller et dépanner l'appliance.

L'appliance divise les différents types d'activités en différents types de journalisation pour simplifier la recherche d'informations sur des activités spécifiques. La plupart d'entre eux sont activés automatiquement par défaut, mais certains doivent être activés manuellement selon les besoins.

Vous activez et gérez les fichiers journaux par le biais d'abonnements aux fichiers journaux. Les abonnements vous permettent de définir les paramètres de création, de personnalisation et de gestion des fichiers journaux.

Les deux principaux types de fichiers journaux généralement utilisés par les administrateurs sont les suivants :

- **Journal d'accès.** Ce journal enregistre toutes les activités de filtrage et d'analyse des proxy Web.

- **Journal de supervision de trafic** Ce journal enregistre toute l'activité du processus de supervision du trafic de la couche 4.

Vous pouvez afficher l'activité actuelle et passée de l'appliance à l'aide de ces types de journaux et d'autres. Des tableaux de référence sont disponibles pour vous aider à interpréter les entrées des fichiers journaux.

Thèmes connexes

- Tâches courantes de journalisation, on page 484
- Types de fichiers journaux, on page 485

Tâches courantes de journalisation

Tâche	Liens vers des rubriques et des procédures connexes
Ajouter et modifier des abonnements aux journaux	Ajout et modification d'abonnements aux journaux, on page 491
Afficher les fichiers journaux	Affichage des fichiers journaux, on page 499
Interpréter les fichiers journaux	Interprétation des entrées de verdict d'analyse des journaux d'accès, on page 513
Personnaliser les fichiers journaux	Personnalisation des journaux d'accès, on page 523
Envoyer les fichiers journaux vers un autre serveur	Transmission des fichiers journaux à un autre serveur, on page 497
Archivage des fichiers journaux	Archivage des fichiers journaux, on page 498

Bonnes pratiques en matière de journalisation

- La réduction du nombre d'abonnements aux journaux améliorera les performances du système.
- La journalisation de moins de détails améliorera les performances du système.

Résolution de problèmes de proxy Web en utilisant les journaux

Par défaut, Secure Web Appliance a un abonnement au journal créé pour les messages de journalisation du proxy Web, appelé « journaux de proxy par défaut ». Cela capture des informations de base sur tous les modules de proxy Web. L'appliance comprend également des types de fichiers journaux pour chaque module de proxy Web afin que vous puissiez lire des informations de débogage plus spécifiques pour chaque module sans encombrer les journaux de proxy par défaut.

Suivez les étapes ci-dessous pour résoudre les problèmes de proxy Web à l'aide des différents journaux disponibles.

Étape 1 Lisez les journaux de proxy par défaut.

Étape 2 Si vous voyez une entrée qui pourrait être liée au problème mais qu'il n'y a pas suffisamment d'informations pour le résoudre, créez un abonnement au journal pour le module de proxy Web spécifique concerné. Les types de journaux de module de proxy Web suivants sont disponibles :

Journaux du moteur de contrôle d'accès	Journaux relatifs à l'environnement de journalisation
Journaux relatifs à l'environnement du moteur AVC	Journaux relatifs à l'environnement d'intégration de McAfee
Journaux de configuration	Journaux du gestionnaire de mémoire
Journaux de gestion des connexions	Journaux de divers modules de proxy
Journaux du module de sécurité des données	Journaux de débogage des demandes
Journaux relatifs à l'environnement du moteur DCA	Journaux du module SNMP
Journaux du gestionnaire de disque	Journaux relatifs à l'environnement d'intégration Sophos
FireAMP	Journaux relatifs à l'environnement WBRS
Journaux de proxy FTP	Journaux du module WCCP
HTTPS Logs (Journaux HTTPS)	Journaux relatifs à l'environnement d'intégration Webcat
Journaux du module de licence	Journaux relatifs à l'environnement d'intégration Webroot

Étape 3 Recréez le problème et lisez le journal du nouveau module de proxy Web pour repérer les entrées pertinentes.

Étape 4 Répétez l'opération au besoin avec les autres journaux du module de proxy Web.

Étape 5 Supprimez les abonnements qui ne sont plus nécessaires.

What to do next

Thèmes connexes

- Types de fichiers journaux, on page 485
- Ajout et modification d'abonnements aux journaux, on page 491

Types de fichiers journaux

Certains types de journaux liés au composant proxy Web ne sont pas activés. Le type de journal principal du proxy Web, appelé « journaux de proxy par défaut », est activé par défaut et capture des informations élémentaires sur tous les modules de proxy Web. Chaque module de proxy Web possède son propre type de journal que vous pouvez activer manuellement au besoin.

Le tableau suivant décrit les types de fichiers journaux Secure Web Appliance.

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux du moteur de contrôle d'accès	Enregistre les messages liés au moteur d'évaluation de la liste de contrôle d'accès (ACL) du proxy Web.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux du moteur Cisco Secure Endpoint	Enregistre des informations sur le contrôle de réputation des fichiers et l'analyse des fichiers (Cisco Secure Endpoint). Voir aussi Fichiers de journalisation , on page 344.	Oui	Oui
Journaux d'audit	Enregistre les événements AAA (Authentication, Authorization et Accounting ou Authentification, Autorisation et Comptabilité). Enregistre toutes les interactions de l'utilisateur avec l'application et les interfaces de ligne de commande, et capture les modifications validées. Voici quelques détails du journal d'audit : • Utilisateur – Connexion • Utilisateur – Échec de connexion, mot de passe incorrect • Utilisateur – Échec de connexion, nom d'utilisateur inconnu • Utilisateur – Échec du compte, expiration de la connexion • Utilisateur – Déconnexion • Utilisateur – Verrouillage • Utilisateur - Activé • Utilisateur – Changement de mot de passe • Utilisateur – Réinitialisation du mot de passe • Utilisateur – Modification de paramètres/du profil de sécurité • Utilisateur – Créé • Utilisateur – Supprimé/modifié • Groupe/rôle – Suppression/modifié • Groupe/rôle – Modification des autorisations	Oui	Oui
Journaux d'accès	Enregistre l'historique du client de proxy Web.	Oui	Oui
Journaux relatifs à l'environnement d'authentification	Enregistre l'historique et les messages d'authentification.	Non	Oui

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux relatifs à l'environnement du moteur AVC	Enregistre les messages liés à la communication entre le proxy Web et le moteur AVC.	Non	Non
Journaux du moteur AVC	Enregistre les messages de débogage du moteur AVC.	Oui	Oui
Journaux d'audit de l'interface de ligne de commande	Enregistre un audit historique de l'activité de l'interface de ligne de commande.	Oui	Oui
Journaux de configuration	Enregistre les messages relatifs au système de gestion de la configuration du proxy Web.	Non	Non
Journaux de gestion des connexions	Enregistre les messages liés au système de gestion des connexions du proxy Web.	Non	Non
Journaux de sécurité des données	Enregistre l'historique du client pour les demandes de chargement évaluées par les filtres de sécurité des données de Cisco.	Oui	Oui
Journaux du module de sécurité des données	Enregistre les messages liés aux filtres de sécurité des données Cisco.	Non	Non
Journaux relatifs à l'environnement du moteur DCA (Dynamic Content Analysis)	Enregistre les messages relatifs à la communication entre le proxy Web et le moteur Cisco Web Usage Controls Dynamic Content Analysis.	Non	Non
Journaux du moteur DCA (Dynamic Content Analysis)	Enregistre les messages liés au moteur Cisco Web Usage Controls Dynamic Content Analysis.	Oui	Oui
Journaux de proxy par défaut	Enregistre les erreurs liées au proxy Web. Il s'agit du plus simple de tous les journaux liés au proxy Web. Pour résoudre des problèmes plus spécifiques liés au proxy Web, créez un abonnement au journal pour le module de proxy Web applicable.	Oui	Oui
Journaux du gestionnaire de disque	Enregistre les messages du proxy Web liés à l'écriture dans le cache sur le disque.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux d'authentification extérieure	Enregistre les messages liés à l'utilisation de la fonction d'authentification extérieure tels que la réussite ou l'échec de la communication avec le serveur d'authentification extérieure Même si l'authentification extérieure est désactivée, ce journal contient des messages concernant les utilisateurs locaux qui ont réussi ou non à se connecter.	Non	Oui
Journaux de commentaires	Enregistre les utilisateurs Web ayant signalé des pages mal classées.	Oui	Oui
Journaux de proxy FTP	Enregistre les messages d'erreur et d'avertissement liés au proxy FTP.	Non	Non
Journaux du serveur FTP	Enregistre tous les fichiers chargés sur et téléchargés à partir de Secure Web Appliance au moyen de FTP.	Oui	Oui
Journaux de l'interface graphique utilisateur (GUI)	Enregistre l'historique des actualisations de page dans l'interface Web. Les journaux de l'interface graphique utilisateur comprennent également des informations sur les transactions SMTP, par exemple des informations sur les rapports planifiés envoyés par courriel par l'appliance.	Oui	Oui
Journaux Haystack	Les journaux Haystack enregistrent le traitement des données de suivi des transactions Web.	Oui	Oui
HTTPS Logs (Journaux HTTPS)	Enregistre les messages de proxy Web propres au proxy HTTPS (lorsque le proxy HTTPS est activé).	Non	Non
Journaux de serveur ISE	Enregistre les informations opérationnelles et relatives aux connexions du serveur ISE.	Oui	Oui
Journaux du module de licence	Enregistre les messages relatifs à la licence du proxy Web et au système de gestion des clés de fonctionnalité.	Non	Non
Journaux relatifs à l'environnement de journalisation	Enregistre les messages relatifs au système de journalisation du proxy Web.	Non	Non
Journaux de journalisation	Enregistre les erreurs liées à la gestion des journaux.	Oui	Oui

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux relatifs à l'environnement d'intégration de McAfee	Enregistre les messages relatifs à la communication entre le proxy Web et le moteur d'analyse McAfee.	Non	Non
Journaux McAfee	Enregistre l'état de l'activité d'analyse de protection contre les programmes malveillants du moteur d'analyse McAfee.	Oui	Oui
Journaux du gestionnaire de mémoire	Enregistre les messages du proxy Web liés à la gestion de toute la mémoire, y compris le cache en mémoire du processus du proxy Web.	Non	Non
Journaux de divers modules de proxy	Enregistre les messages de proxy Web qui sont principalement utilisés par les développeurs ou l'assistance client.	Non	Non
Journaux du démon d'AnyConnect Secure Mobility	Enregistre l'interaction entre Secure Web Appliance et le client AnyConnect, y compris la vérification de l'état.	Oui	Oui
Journaux NTP (Network Time Protocol)	Enregistre les modifications de l'horloge système effectuées par le protocole Network Time Protocol.	Oui	Oui
Journaux du démon d'hébergement de fichiers PAC	Enregistre l'utilisation du fichier de configuration automatique de proxy (PAC) par les clients.	Oui	Oui
Journaux de contournement de proxy	Enregistre les transactions qui contournent le proxy Web.	Non	Oui
Journaux de rapports	Enregistre un historique de la création de rapports.	Oui	Oui
Journaux des requêtes de rapports	Enregistre les erreurs liées à la génération de rapports.	Oui	Oui
Journaux de débogage des demandes	Enregistre des informations de débogage très détaillées sur une transaction HTTP spécifique à partir de tous les types de journaux de module de proxy Web. Vous souhaiterez peut-être créer cet abonnement au journal pour résoudre un problème de proxy avec une transaction particulière sans créer tous les autres abonnements aux journaux de proxy. **Remarque :** Vous pouvez créer cet abonnement à ce journal uniquement à l'aide de l'interface de ligne de commande.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux d'authentification	Enregistre les messages relatifs à la fonction de contrôle d'accès.	Oui	Oui
Journaux SHD (System Health Daemon)	Enregistre un historique de l'état des services du système et un historique des redémarrages inattendus de démon.	Oui	Oui
Journaux SNMP	Enregistre les messages de débogage liés au moteur de gestion réseau SNMP.	Oui	Oui
Journaux du module SNMP	Enregistre les messages de proxy Web liés à l'interaction avec le système de supervision SNMP.	Non	Non
Journaux relatifs à l'environnement d'intégration Sophos	Enregistre les messages liés à la communication entre le proxy Web et le moteur d'analyse Sophos.	Non	Non
Journaux Sophos	Enregistre l'état de l'activité de contrôle des programmes malveillants par le moteur d'analyse Sophos.	Oui	Oui
Journaux d'état	Enregistre les informations relatives au système, telles que les téléchargements de clés de fonctionnalité.	Oui	Oui
Journaux du système	Enregistre le DNS, les erreurs et les activités de validation.	Oui	Oui
Journaux d'erreurs de la supervision du trafic	Enregistre les erreurs de capture et de l'interface de supervision du trafic de la couche 4.	Oui	Oui
Journaux de supervision du trafic	Enregistre les sites ajoutés aux listes de blocage et d'autorisation de la supervision du trafic de la couche 4.	Non	Oui
Journaux UDS (User Discovery Service)	Enregistre les données sur la façon dont le proxy Web détecte le nom d'utilisateur sans effectuer d'authentification réelle. Il contient des informations sur l'interaction avec Cisco Adaptive Security Appliance pour Secure Mobility, ainsi que sur l'intégration au serveur Novell eDirectory pour l'identification transparente des utilisateurs.	Oui	Oui
Journaux du programme de mise à jour	Enregistre un historique de WBRS et d'autres mises à jour.	Oui	Oui

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux W3C	Enregistre l'historique du client de proxy Web dans un format compatible avec W3C. Pour en savoir plus, consultez Fichiers journaux des accès conformes aux normes W3C, on page 521.	Oui	Non
Journaux WBNP (participation au réseau SensorBase)	Enregistre un historique des chargements de participation au réseau Cisco SensorBase dans le réseau SensorBase.	Non	Oui
Journaux relatifs à l'environnement WBRS (Score de réputation Web)	Enregistre les messages liés à la communication entre le proxy Web et les filtres de réputation Web.	Non	Non
Journaux du module WCCP	Enregistre les messages du proxy Web liés à la mise en œuvre de WCCP.	Non	Non
Journaux relatifs à l'environnement d'intégration Webcat	Enregistre les messages liés à la communication entre le proxy Web et le moteur de filtrage d'URL associé à Cisco Web Usage Controls.	Non	Non
Journaux relatifs à l'environnement d'intégration Webroot	Enregistre les messages liés à la communication entre le proxy Web et le moteur d'analyse Webroot.	Non	Non
Journaux Webroot	Enregistre l'état de l'activité d'analyse de protection contre les programmes malveillants du moteur d'analyse Webroot.	Oui	Oui
Journaux d'accusé de réception de la page de bienvenue	Enregistre un historique des clients Web qui ont cliqué sur le bouton Accept (Accepter) dans la page d'accusé de réception de l'utilisateur final.	Oui	Oui

Ajout et modification d'abonnements aux journaux

Vous pouvez créer plusieurs abonnements à des journaux pour chaque type de fichier journal. Les abonnements comprennent des détails de configuration pour l'archivage et le stockage, notamment les suivants :

- Les paramètres de renouvellement, qui déterminent quand les fichiers journaux sont archivés.
- Paramètres de compression des journaux archivés
- Les paramètres de récupération des journaux archivés, qui spécifient si les journaux sont archivés sur un serveur distant ou stockés sur l'appliance.

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Pour ajouter un abonnement à la journalisation, cliquez sur **Add Log Subscription** (Ajouter un abonnement au journal). Ou, pour modifier un abonnement à un journal, cliquez sur le nom du fichier journal dans le champ Log Name (Nom du journal).

Étape 3 Configurez l'abonnement :

Option	Description
Log Type (Type de journal)	Une liste des types de fichiers journaux disponibles auxquels vous pouvez vous abonner. Les autres options de la page peuvent changer en fonction du type de fichier journal que vous choisissez. **Note** Le type de journal Request Debug Logs (Demande de journaux de débogage) ne peut être souscrit que par l'intermédiaire de l'interface de ligne de commande et n'apparaît pas dans cette liste.
Log Name (Nom du journal)	Nom utilisé pour désigner l'abonnement sur Secure Web Appliance. Ce nom est également utilisé pour le répertoire des journaux qui stockera les fichiers journaux de l'abonnement. Saisissez uniquement des caractères ASCII ([0-9], [AZ], [az] et _).
Rollover by File Size (Renouvellement par taille de fichier)	La taille maximale de fichier que le fichier journal actuel peut atteindre avant d'être archivé et qu'un nouveau fichier journal ne démarre. Entrez une valeur comprise entre 100 Ko et 10 Go.
Rollover by Time (Renouvellement par heure)	Intervalle de temps maximal avant l'archivage du fichier journal actuel et le démarrage d'un nouveau fichier journal. Les types d'intervalles suivants sont disponibles : • **Aucun.** AsyncOS n'effectue un remplacement que lorsque le fichier journal atteint la taille maximale de fichier. • **Custom Time Interval.** (Intervalle personnalisé) AsyncOS effectue un renouvellement après un laps de temps spécifié depuis le renouvellement précédent. Indiquez le nombre de jours, d'heures, de minutes et de secondes entre les renouvellements en utilisant d , h , m et s comme suffixes. • **Renouvellement quotidien.** AsyncOS effectue un renouvellement tous les jours à une heure spécifiée. Séparez les heures multiples pendant une journée par une virgule. Utilisez un astérisque (*) dans l'heure pour que le renouvellement se produise toutes les heures de la journée. Vous pouvez également utiliser un astérisque pour remplacer chaque minute d'une heure. • **Weekly Rollover** (Renouvellement hebdomadaire). AsyncOS effectue un renouvellement un ou plusieurs jours de la semaine à une heure spécifiée.
Log Style (Style de journal) (Journaux d'accès)	Indique le format du journal à utiliser, Squid, Apache ou Squid Details.

Option	Description

Custom Fields (Champs personnalisés)
 	
(Journaux d'accès)
	Vous permet d'inclure des informations personnalisées dans chaque entrée du journal des accès.
	
	La syntaxe de saisie des spécificateurs de format dans le champ personnalisé est la suivante :
	
	`<format_specifier_1> <format_specifier_2> ...`
	
	Par exemple : `%a %b %E`
	
	Vous pouvez ajouter des jetons avant les spécificateurs de format pour afficher un texte de description dans le fichier journal des accès. Par exemple :
	
	`client_IP %a body_bytes %b error_type %E`
	
	où `IP_client` est le jeton de description du spécificateur de format de journal `%a`, etc.

File Name (Nom de fichier)	Nom des fichiers journaux. Les fichiers journaux actuels sont dotés d'une extension `.c`, et les fichiers journaux renouvelés sont accompagnés de l'horodatage de création du fichier et d'une extension `.s`.
Log Fields (Champs de journal) (Journaux d'accès W3C)	Vous permet de choisir les champs que vous souhaitez inclure dans le journal des accès W3C. Sélectionnez un champ dans la liste des champs disponibles ou saisissez un champ dans la zone Custom Field (Champ personnalisé), puis cliquez sur Add (Ajouter). L'ordre dans lequel les champs apparaissent dans la liste Selected Log Fields (Champs de journal sélectionnés) détermine l'ordre des champs dans le fichier du journal d'accès W3C. Vous pouvez modifier l'ordre des champs à l'aide des boutons **Déplacement vers le haut** et **Déplacement vers le bas**. Vous pouvez supprimer un champ en le sélectionnant dans la liste Selected Log Fields (Champs de journal sélectionnés) et en cliquant sur **Remove** (Supprimer). Vous pouvez saisir plusieurs champs définis par l'utilisateur dans la zone Custom Fields (Champs personnalisés) et les ajouter simultanément à condition que chaque entrée soit séparée par une nouvelle ligne [cliquez sur Enter (Entrée)] avant de cliquer sur **Add** (Ajouter). Lorsque vous modifiez les champs de journal inclus dans un abonnement à un journal W3C, l'abonnement au journal est automatiquement renouvelé. Cela permet à la dernière version du fichier journal d'inclure les nouveaux en-têtes de champ corrects Vous pouvez anonymiser les champs de journalisation *c-ip*, *cs-username*ou *cs-auth-group* des journaux W3C, au besoin. Cochez la case **Anonymization** (Anonymisation) pour anonymiser les champs *c-ip*, *cs-username* et *cs-auth-group*. Une fois que vous avez sélectionné la case, les noms de champ sont remplacés par *ca-ip*, *cs-a-username* et *cs-a-auth-group*, respectivement. **Note** Vous devez activer l'anonymisation uniquement si le serveur externe vers lequel les fichiers journaux sont envoyés est compatible pour gérer la fonction d'anonymisation. Après la création du journal, vous pouvez désanonymiser les champs anonymisés, si nécessaire. Voir la section Désanonymisation des champs de journalisation W3C, on page 496.

Option	Description
Passphrase for Anonymization (Phrase secrète pour l'anonymisation) (Journaux d'accès W3C)	Vous permet de créer une phrase secrète pour chiffrer les valeurs des champs. Cette zone sera activée uniquement lorsque vous choisirez d'anonymiser les champs de journalisation *c-ip*, *cs-username* ou *cs-auth-group*. **Note** Le système applique les règles de phrase secrète lors de sa configuration pour l'anonymisation. Pour générer automatiquement une phrase secrète, cochez la case à côté de **Auto Generate Passphrase** (Générer automatiquement la phrase secrète) et cliquez sur **Generate** (Générer). **Note** Si vous avez plusieurs périphériques, ils doivent tous définir la même phrase secrète.
Log Compression (Compression journal)	Indique si les fichiers remplacés sont compressés. AsyncOS compresse les fichiers de journalisation au format gzip.
Log Exclusions (Exclusions de journaux) (facultatif) (Journaux d'accès)	Vous permet de préciser les codes d'état HTTP (4xx ou 5xx uniquement) pour exclure les transactions associées d'un journal des accès ou du journal des accès W3C. Par exemple, la saisie de 401 filtrera les demandes d'échec d'authentification qui ont ce numéro de transaction.
Log Level (Niveau du journal)	Spécifie le niveau de détail des entrées de journal. Choisissez parmi : • **Critical** (Critique). Inclut uniquement les erreurs. Il s'agit du paramètre le moins détaillé; il équivaut au niveau d'alerte du journal système. • **Warning** (Avertissement). Inclut erreurs et avertissements. Ce niveau de journalisation est équivalent au niveau d'avertissement du journal système. • **Information**. Inclut les erreurs, les avertissements et les opérations supplémentaires du système. Il s'agit du niveau de détail par défaut et il équivaut au niveau « Info » du journal système. • **Debug** (Débogage). Comprend des données utiles pour le débogage des problèmes du système. Utilisez le niveau de journalisation de débogage lorsque vous essayez de découvrir la cause d'une erreur. Utilisez ce paramètre temporairement, puis revenez au niveau par défaut. Ce niveau de journalisation est équivalent au niveau de débogage du journal système. • **Trace** (Suivi). Il s'agit du paramètre le plus détaillé. Ce niveau comprend un enregistrement complet des opérations et des activités du système. Le niveau de journalisation Trace (Suivi) est recommandé uniquement pour les développeurs. L'utilisation de ce niveau entraîne une grave dégradation des performances du système et n'est pas recommandée. Ce niveau de journalisation est équivalent au niveau de débogage du journal système. **Note** Des paramètres plus détaillés créent des fichiers journaux plus volumineux et ont un impact plus important sur les performances du système.
Retrieval Method (Méthode de récupération)	Spécifie où les fichiers journaux reportés sont stockés et comment ils sont récupérés pour la lecture. Vous trouverez ci-dessous une description des méthodes disponibles.

Option	Description
Retrieval Method (Méthode de récupération) : FTP sur l'appliance	La méthode FTP sur l'appliance (équivalente à interrogation FTP) nécessite un client FTP distant accédant à l'appliance pour récupérer les fichiers journaux à l'aide du nom d'utilisateur et de la phrase secrète d'un administrateur ou opérateur. Lorsque vous choisissez cette méthode, vous devez saisir le nombre maximal de fichiers journaux à stocker sur l'appliance. Lorsque le nombre maximal est atteint, le système supprime le fichier le plus ancien. Il s'agit de la méthode de récupération par défaut.
Retrieval Method (Méthode de récupération) : FTP sur serveur distant	La méthode FTP sur serveur distant (équivalente au transfert FTP) envoie régulièrement les fichiers journaux sur un serveur FTP sur un ordinateur distant. Lorsque vous choisissez cette méthode, vous devez saisir les informations suivantes : • Nom d'hôte du serveur FTP • Répertoire sur le serveur FTP où stocker le fichier journal • Nom d'utilisateur et phrase secrète d'un utilisateur qui est autorisé à se connecter au serveur FTP **Note** AsyncOS pour le Web prend uniquement en charge le mode passif pour les serveurs FTP distants. Les fichiers journaux ne peuvent pas être transférés vers un serveur FTP en mode actif.
Retrieval Method (Méthode de récupération) : SCP sur serveur distant	La méthode SCP sur serveur distant (équivalente à la méthode SCP Push) envoie régulièrement les fichiers journaux à l'aide du protocole de copie sécurisée vers un serveur SCP distant. Cette méthode nécessite un serveur SSH SCP sur un ordinateur distant utilisant le protocole SSH2. L'abonnement nécessite un nom d'utilisateur, une clé SSH et un répertoire de destination sur l'ordinateur distant. Les fichiers journaux sont transférés selon un calendrier de renouvellement que vous définissez. Lorsque vous choisissez cette méthode, vous devez saisir les informations suivantes : • Nom d'hôte du serveur SCP • Répertoire sur le serveur SCP pour stocker le fichier journal • Nom d'utilisateur d'un utilisateur qui est autorisé à se connecter au serveur SCP **Note** Actuellement, nous prenons uniquement en charge SSH-RSA et SSH-DSS en mode non FIPS, ainsi que SSH-RSA en mode FIPS.

Option	Description
Retrieval Method (Méthode de récupération) : Syslog Push	Vous ne pouvez choisir syslog que pour les journaux texte. La méthode Syslog Push envoie des messages de journal à un serveur syslog distant sur le port 514. Cette méthode est conforme à la RFC 3164. Lorsque vous choisissez cette méthode, vous devez saisir les informations suivantes : • Nom d'hôte du serveur Syslog • Protocole à utiliser pour la transmission, UDP ou TCP • Taille maximale des messages Les valeurs correctes pour UDP sont comprises entre 1024 et 9216. Les valeurs correctes pour TCP sont comprises entre 1024 et 65 535. La taille maximale des messages dépend de la configuration du serveur syslog. • Facilité à utiliser avec le journal

Étape 4 Envoyez et validez vos modifications.

What to do next

Si vous avez choisi SCP comme méthode de récupération, remarquez que l'appliance affiche une clé SSH, que vous ajouterez à l'hôte du serveur SCP. Consultez Transmission des fichiers journaux à un autre serveur, on page 497.

Thèmes connexes

- Types de fichiers journaux, on page 485
- Noms des fichiers journaux et structure des répertoires de l'appliance, on page 498

Désanonymisation des champs de journalisation W3C

Si vous avez activé la fonction d'anonymisation pour les valeurs de champ (*c-ip, cs-username* et *cs-auth-group*) lors de l'abonnement au journal, le serveur de journaux de destination recevra les valeurs anonymisées (*c-a-ip*, *cs-a-username* et *cs-a-auth-group*) de ces champs de journal et non des valeurs réelles. Si vous souhaitez afficher les valeurs réelles, vous devez désanonymiser les champs du journal.

Vous pouvez désanonymiser les valeurs des champs de journalisation *ca-ip*, *cs-a-username* et *cs-a-auth-group* qui sont anonymisées lors de l'ajout de l'abonnement au journal W3C.

Étape 1 Choisissez **System Administration** > **Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur **Deanonymization** (Désanonymisation) dans la colonne Delonymization (Désanonymisation) correspondant au journal pour lequel vous souhaitez désanonymiser les champs anonymisés.

Étape 3 Dans la zone **Method** (Méthode), choisissez l'une des méthodes suivantes pour saisir le texte chiffré à désanonymiser.

- Paste encrypted text (Coller le texte chiffré) : collez uniquement le texte chiffré dans le champ de texte anonymisé. Vous pouvez saisir un maximum de 500 entrées dans ce champ. Vous devez séparer les entrées multiples par une virgule.
- Upload File (Charger un fichier) : choisissez un fichier qui contient le texte chiffré. Le fichier peut contenir un maximum de 1 000 entrées. Le fichier doit être au format CSV. Le système prend en charge les espaces, les retours à la ligne, les tabulations et les points-virgules comme séparateurs de champ.

Remarque Si vous avez modifié la phrase secrète, vous devez l'entrer dans l'ancienne pour anonymiser les anciennes données.

Étape 4 Cliquez sur **Deanonymize** (Désanonymiser) et le tableau des résultats de la désanonymisation affiche les valeurs des champs de journal désanonymisées.

Transmission des fichiers journaux à un autre serveur

Before you begin

Créez ou modifiez l'abonnement au journal souhaité en choisissant SCP comme méthode de récupération.
Ajout et modification d'abonnements aux journaux, on page 491

Étape 1 Ajouter des clés au système distant :

a) Accédez à l'interface de ligne de commande.
b) Utilisez la commande `logconfig -> hostkeyconfig`.
c) Utilisez les commandes ci-dessous pour afficher les clés :

Commande	Description
Host (Hôte)	Affichez les clés d'hôte du système. Il s'agit de la valeur à placer dans le fichier « known_hosts » du système distant.
User (Utilisateur)	Affiche la clé publique du compte système qui pousse les journaux vers l'ordinateur distant. Il s'agit de la même clé qui est affichée lors de la configuration d'un abonnement de transmission SCP. Il s'agit de la valeur à placer dans le fichier « autorized_keys » du système distant.

d) Ajoutez ces clés au système distant.

Étape 2 Toujours dans l'interface de ligne de commande, ajoutez la clé d'hôte publique SSH du serveur distant à l'appliance :

Commande	Description
New (Nouvelle)	Ajoutez une nouvelle clé.
Fingerprint (Empreinte)	Affichez les empreintes de la clé d'hôte du système.

Étape 3 Validez vos modifications.

Archivage des fichiers journaux

AsyncOS archive (renouvelle) les abonnements aux journaux lorsqu'un fichier journal actuel atteint la limite spécifiée par l'utilisateur de taille de fichier maximale ou le temps maximal depuis le dernier renouvellement.

Ces paramètres d'archivage sont inclus dans les abonnements aux journaux :

- Rollover by File Size (Renouvellement par taille de fichier)
- Rollover by Time (Renouvellement par heure)
- Log Compression (Compression journal)
- Retrieval Method (Méthode de récupération)

Vous pouvez également archiver manuellement (renouveler) les fichiers journaux.

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cochez la case dans la colonne Rollover (Renouvellement) des abonnements aux journaux que vous souhaitez archiver ou cochez la case **All** (Tous) pour sélectionner tous les abonnements.

Étape 3 Cliquez sur **Rollover Now** (Renouveler maintenant) pour archiver les journaux sélectionnés.

What to do next

Thèmes connexes

- Ajout et modification d'abonnements aux journaux, on page 491
- Noms des fichiers journaux et structure des répertoires de l'appliance, on page 498

Noms des fichiers journaux et structure des répertoires de l'appliance

L'appliance crée un répertoire pour chaque abonnement à un journal en fonction du nom d'abonnement au journal. Le nom du fichier journal dans le répertoire est composé des informations suivantes :

- Nom du fichier journal spécifié dans l'abonnement au journal
- Horodatage du démarrage du fichier journal
- Un code d'état à un caractère, soit .c (signifiant actuel) ou .s (signifiant enregistré)

Le nom de fichier des journaux est créé en utilisant la formule suivante :

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

Note Vous ne devez transférer que les fichiers journaux avec l'état enregistré.

Lecture et interprétation des fichiers journaux

Vous pouvez consulter l'activité du fichier journal actuel pour surveiller et dépanner Secure Web Appliance. Cela s'effectue à l'aide de l'interface de l'appliance.

Vous pouvez également lire des fichiers archivés pour un enregistrement de l'activité passée. Cela peut se faire à l'aide de l'interface de l'appliance si les fichiers archivés sont stockés sur l'appliance; sinon, elles doivent être lues à partir de leur emplacement de stockage externe à l'aide d'une méthode appropriée.

Chaque élément d'information d'un fichier journal est représenté par une variable de champ. En identifiant quels champs représentent quels éléments d'information, vous pouvez rechercher la fonction du champ et interpréter le contenu du fichier journal. Pour les journaux d'accès conformes W3C, l'en-tête du fichier indique les noms des champs dans l'ordre dans lequel ils apparaissent dans les entrées du journal. Pour les journaux d'accès standard, cependant, vous devez consulter la documentation concernant ce type de journal pour obtenir des renseignements sur l'ordre des champs.

Thèmes connexes

- Affichage des fichiers journaux, on page 499.
- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500.
- Interprétation des journaux d'accès W3C, on page 521.
- Interprétation des journaux de supervision du trafic, on page 528.
- Champs et balises des fichiers journaux, on page 528.

Affichage des fichiers journaux

Before you begin

Sachez que cette méthode d'affichage est destinée aux fichiers journaux stockés sur l'appliance. Le processus d'affichage des fichiers stockés à l'externe dépasse le cadre de cette documentation.

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur le nom de l'abonnement au journal dans la colonne Log Files (Fichiers journaux) de la liste des abonnements aux journaux.

Étape 3 Lorsque vous y êtes invité, saisissez le nom d'utilisateur et la phrase secrète de l'administrateur pour accéder à l'appliance.

Étape 4 Une fois connecté, cliquez sur l'un des fichiers journaux pour l'afficher dans votre navigateur ou l'enregistrer sur le disque.

Étape 5 Actualisez le navigateur pour des résultats à jour.

Note Si un abonnement à un journal est compressé, téléchargez-le, décompressez-le, puis ouvrez-le.

What to do next

Thèmes connexes

Informations sur le proxy Web dans les fichiers journaux d'accès

Les fichiers journaux d'accès fournissent un enregistrement descriptif de toutes les activités de filtrage et d'analyse des proxys Web. Les entrées du fichier journal d'accès affichent un enregistrement de la façon dont l'appliance a traité chaque transaction.

Les journaux d'accès sont disponibles en deux formats : le format standard et celui conforme au W3C. Les fichiers journaux conformes au W3C sont plus personnalisables en ce qui concerne leur contenu et leur disposition que les journaux d'accès standard.

Le texte suivant est un exemple d'entrée de fichier journal des accès pour une transaction unique :

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy-NONE
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-",""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e”>
 -
```

Spécificateur de format	Valeur de champ	Description du champ
%t	`1278096903.150`	Horodatage depuis UNIX.
%e	`97`	Temps écoulé (latence) en millisecondes.
%a	`172.xx.xx.xx`	Adresse IP du client. **Remarque :** Vous pouvez choisir de masquer l'adresse IP dans les journaux d'accès à l'aide de la commande sur l'interface de ligne de commande advancedproxyconfig > authentication.
%w	`TCP_MISS`	Code de résultat de transaction. Pour en savoir plus, consultez Fichiers journaux des accès conformes aux normes W3C, on page 521.
%h	`200`	Code de réponse HTTP.
%s	`8187`	Taille de la réponse (en-têtes + corps)

Spécificateur de format	Valeur de champ	Description du champ
%1r %2r	`GET http://my.site.com/`	Première ligne de la demande. Remarque : Lorsque la première ligne de la demande concerne une transaction FTP native, certains caractères spéciaux du nom de fichier sont codés sous forme d'URL dans les journaux d'accès. Par exemple, le symbole « @ » est inscrit « %40 » dans les journaux d'accès. Les caractères suivants sont codés en mode URL : & # % + , : ; = @ ^ { } [ ]
%A	–	Nom d'utilisateur authentifié **Remarque :** Vous pouvez choisir de masquer le nom d'utilisateur dans les journaux d'accès à l'aide de la commande sur l'interface de ligne de commande `advancedproxyconfig > authentication`.
%H	`DIRECT`	Code qui décrit quel serveur a été contacté pour récupérer le contenu de la demande. Les valeurs les plus courantes comprennent : • **NONE.** Le proxy Web avait le contenu, donc il n'a contacté aucun autre serveur pour récupérer le contenu. • **DIRECT.** Le proxy Web est allé au serveur nommé dans la demande pour obtenir le contenu. • **DEFAULT_PARENT.** Le proxy Web s'est rendu chez son proxy parent principal ou sur un serveur DLP externe pour obtenir le contenu.
%d	`my.site.com`	Adresse IP de la source de données ou du serveur.
%c	`text/plain`	Type de corps de réponse MIME.

Spécificateur de format	Valeur de champ	Description du champ
%D	`DEFAULT_CASE_11`	Balise de décision ACL. **Remarque :** La fin de la balise de décision ACL comprend un numéro généré dynamiquement que le proxy Web utilise en interne. Vous pouvez ignorer ce numéro. Pour en savoir plus, consultez Balises de décision ACL, on page 505.
S.O. (faisant partie de la balise de décision ACL)	`PolicyGroupName`	Nom du groupe de politiques responsable de la décision finale concernant cette transaction (politique d'accès, politique de déchiffrement ou politique de sécurité des données). Lorsque la transaction correspond à une politique globale, cette valeur est « DefaultGroup ». Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`Identité`	Nom du groupe de politiques d'identité Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`OutboundMalwareScanningPolicy`	Nom du groupe de politiques d'analyse des programmes malveillants sortants. Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).

Spécificateur de format	Valeur de champ	Description du champ
S.O. (faisant partie de la balise de décision ACL)	`DataSecurityPolicy`	Nom du groupe de politiques de sécurité des données de Cisco. Lorsque la transaction correspond à la politique de sécurité des données globale de Cisco, cette valeur est « DefaultGroup ». Ce nom de groupe de politiques ne s'affiche que lorsque les filtres de sécurité des données Cisco sont activés. « NONE » s'affiche lorsqu'aucune politique de sécurité des données n'a été appliquée. Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`ExternalDLPPolicy`	Nom du groupe de politiques DLP externe. Lorsque la transaction correspond à la politique de DLP externe globale, cette valeur est « DefaultGroup ». « NONE » s'affiche lorsqu'aucune politique DLP externe n'a été appliquée. Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`RoutingPolicy`	Le nom du groupe de politiques de routage est *ProxyGroupName/ProxyServerName*. Lorsque la transaction correspond à la politique de routage globale, cette valeur est « DefaultRouting ». Lorsqu'aucun serveur proxy en amont n'est utilisé, cette valeur est « DIRECT ». Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).

Spécificateur de format	Valeur de champ	Description du champ
%Xr	<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,""-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	Informations sur le verdict de l'analyse. À l'intérieur des crochets en angle, les journaux d'accès comprennent des renseignements sur les verdicts provenant de divers moteurs d'analyse. **Note** Dans AsyncOS version 11.8 et ultérieure, l'identifiant de catégorie d'URL apparaît entre guillemets doubles. Par exemple, « IW_comp ». Pour en savoir plus sur les valeurs incluses entre les crochets, consultez Interprétation des entrées de verdict d'analyse des journaux d'accès, on page 513 et Valeurs de verdict de la recherche de programmes malveillants, on page 543.
%?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?% < User-Agent:%!%-%	–	Agent utilisateur suspect.

Codes de résultats de transactions

Les codes de résultats de transaction dans le fichier journal des accès décrivent comment l'appliance résout les demandes des clients. Par exemple, si une demande pour un objet peut être résolue à partir du cache, le code de résultat est `TCP_HIT`. Toutefois, si l'objet ne se trouve pas dans le cache et que l'appliance extrait l'objet d'un serveur d'origine, le code de résultat est `TCP_MISS`. Le tableau suivant décrit les codes de résultats de transactions.

Code de résultat	Description
`TCP_HIT`	L'objet demandé a été récupéré à partir du cache disque.
`TCP_IMS_HIT`	Le client a envoyé une demande IMS (IF-Modified-Since) pour un objet et l'objet a été trouvé dans le cache. Le proxy répond par une réponse 304.
`TCP_MEM_HIT`	L'objet demandé a été récupéré de la mémoire cache.
`TCP_MISS`	L'objet n'a pas été trouvé dans le cache, il a donc été récupéré du serveur d'origine.

Code de résultat	Description
TCP_REFRESH_HIT	L'objet se trouve dans le cache, mais il a expiré. Le proxy a envoyé une demande IMS (IF-Modified-Since) au serveur d'origine et le serveur a confirmé que l'objet n'a pas été modifié. Par conséquent, l'appliance a récupéré l'objet à partir du cache disque ou de la mémoire cache.
TCP_CLIENT_REFRESH_MISS	Le client a envoyé une demande « ne pas récupérer la réponse du cache » en émettant l'en-tête « Pragma: no-cache ». En raison de cet en-tête du client, l'appliance a récupéré l'objet du serveur d'origine.
TCP_DENIED	La demande du client a été refusée en raison des politiques d'accès.
UDP_MISS	L'objet a été récupéré du serveur d'origine.
NONE	Une erreur s'est produite dans la transaction. Par exemple, une défaillance DNS ou un délai d'attente de passerelle.

Balises de décision ACL

Une balise de décision ACL est un champ d'une entrée du journal d'accès qui indique comment le proxy Web a traité la transaction. Elle contient des informations provenant des filtres de réputation Web, des catégories d'URL et des moteurs d'analyse.

Note La fin de la balise de décision ACL comprend un numéro généré dynamiquement que le proxy Web utilise en interne pour augmenter les performances. Vous pouvez ignorer ce numéro.

Le tableau suivant décrit les valeurs des balises de décision d'une liste de contrôle d'accès (ACL).

Balise de décision ACL	Description
ALLOW_ADMIN_ERROR_PAGE	Le proxy Web a autorisé la transaction vers une page de notification et vers tout logo utilisé sur cette page.
ALLOW_CUSTOMCAT	Le proxy Web a autorisé la transaction en fonction des paramètres du filtrage de catégories d'URL personnalisées pour le groupe de politiques d'accès.
ALLOW_REFERER	Le proxy Web a autorisé la transaction en fonction d'une dispense de contenu intégré ou référé.
ALLOW_WBRS	Le proxy Web a autorisé la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques d'accès.

Balise de décision ACL	Description
AMP_FILE_VERDICT	Valeur représentant un verdict à partir du serveur de réputation Cisco Secure Endpoint pour le fichier : • 1 – Inconnu • 2 – Sain • 3 – Malveillant • 4 – Impossible à analyser

Balise de décision ACL	Description
ARCHIVESCAN_ALLCLEAR ARCHIVESCAN_BLOCKEDFILETYPE ARCHIVESCAN_NESTEDTOODEEP ARCHIVESCAN_UNKNOWNFMT ARCHIVESCAN_UNSCANABLE ARCHIVESCAN_FILETOOBIG	**Verdict de l'analyse des archives** ARCHIVESCAN_ALLCLEAR : aucun type de fichier n'est bloqué dans l'archive inspectée. ARCHIVESCAN_BLOCKEDFILETYPE : un type de fichier est bloqué dans l'archive inspectée. Le champ suivant de l'entrée de journal [Verdict Detail (Détails du verdict)] fournit des détails, notamment le type de fichier bloqué et le nom du fichier bloqué. ARCHIVESCAN_NESTEDTOODEEP : l'archive est bloquée, car elle contient plus d'archives « encapsulées » ou imbriquées que le maximum configuré. Le champ Verdict Detail (Détails du verdict) contient la mention « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). ARCHIVESCAN_UNKNOWNFMT : l'archive est bloquée, car elle contient un type de fichier de format inconnu. Le détail du verdict est « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). ARCHIVESCAN_UNSCANABLE : l'archive est bloquée, car elle contient un fichier qui ne peut pas être analysé. Le détail du verdict est « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). ARCHIVESCAN_FILETOOBIG : l'archive est bloquée, car sa taille dépasse la limite maximale configurée. Le détail du verdict est « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). **Détails du verdict de l'analyse des archives** Le champ suivant le champ Verdict dans l'entrée du journal fournit des renseignements supplémentaires sur le verdict, tels que le type de fichier bloqué et le nom du fichier bloqué, « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée) ou « - » pour indiquer que l'archive ne contient aucun type de fichier bloqué. Par exemple, si un fichier d'archive pouvant être inspectée est bloqué (ARCHIVESCAN_BLOCKEDFILETYPE) en fonction des paramètres Access Policy: Custom Objects Blocking (Politique d'accès : Blocage d'objets personnalisés), l'entrée Verdict Detail (Détails du verdict) comprend le type de fichier bloqué et le nom du fichier bloqué. Reportez-vous aux sections Politiques d'accès : blocage d'objets, on page 262 et Paramètres d'inspection des archives, on page 264 pour en savoir plus sur l'inspection des archives.
BLOCK_ADC	Transaction bloquée en fonction des paramètres d'application configurés pour le groupe de politiques d'accès.
BLOCK_ADMIN	Transaction bloquée en fonction de certains paramètres par défaut pour le groupe de politiques d'accès.

Balise de décision ACL	Description
BLOCK_ADMIN_CONNECT	Transaction bloquée en fonction du port TCP de la destination, comme défini dans le paramètre HTTP CONNECT Ports (Ports HTTP CONNECT) pour le groupe de politiques d'accès.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transaction bloquée en fonction de l'agent utilisateur, comme défini dans le paramètre Block Custom User Agents (Bloquer les agents utilisateur personnalisés) pour le groupe de politiques d'accès.
BLOCK_ADMIN_TUNNELING	Le proxy Web a bloqué la transaction en fonction de la tunnellisation du trafic non HTTP sur les ports HTTP pour le groupe de politiques d'accès.
BLOCK_ADMIN_HTTPS_ NonLocalDestination	Transaction bloquée; le client a essayé de contourner l'authentification en utilisant le port SSL comme proxy explicite. Pour éviter cela, si une connexion SSL est établie avec le Secure Web Appliance même, seules les demandes adressées au nom d'hôte de redirection Secure Web Appliance réel sont autorisées.
BLOCK_ADMIN_IDS	Transaction bloquée en fonction du type MIME du corps de la demande, comme défini dans le groupe de politique de sécurité des données.
BLOCK_ADMIN_FILE_TYPE	Transaction bloquée en fonction du type de fichier, comme défini dans le groupe de politiques d'accès.
BLOCK_ADMIN_PROTOCOL	Transaction bloquée sur la base du protocole défini dans le paramètre Block Protocols (Bloquer les protocoles) pour le groupe de politiques d'accès.
BLOCK_ADMIN_SIZE	Transaction bloquée en fonction de la taille de la réponse, comme défini dans les paramètres Object Size (Taille d'objet) pour le groupe de politiques d'accès.
BLOCK_ADMIN_SIZE_IDS	Transaction bloquée en fonction de la taille du contenu du corps de la demande, comme défini dans le groupe de politique de sécurité des données.
BLOCK_AMP_RESP	Le proxy Web a bloqué la réponse en fonction des paramètres Cisco Secure Endpoint du groupe de politiques d'accès.
BLOCK_AMW_REQ	Le proxy Web a bloqué la demande en fonction des paramètres de la protection contre les programmes malveillants pour le groupe de politiques d'analyse des programmes malveillants sortants. Le corps de la demande a produit un verdict positif quant à la présence de programmes malveillants.
BLOCK_AMW_RESP	Le proxy Web a bloqué la réponse en fonction des paramètres de la solution contre les programmes malveillants pour le groupe des politiques d'accès.

Balise de décision ACL	Description
BLOCK_AMW_REQ_URL	Le proxy Web soupçonne que l'URL contenue dans la requête HTTP n'est pas sécurisée. Il a donc bloqué la transaction au moment de la demande en fonction des paramètres contre les programmes malveillants du groupe des politiques d'accès.
BLOCK_AVC	Transaction bloquée en fonction des paramètres d'application configurés pour le groupe de politiques d'accès.
BLOCK_CONTENT_UNSAFE	Transaction bloquée en fonction des paramètres d'évaluation du contenu du site pour le groupe de politiques d'accès. La demande du client visait un contenu pour adultes et la politique est configurée pour bloquer le contenu pour adultes.
BLOCK_CONTINUE_CONTENT_ UNSAFE	Transaction bloquée et affichage de la page Warn and Continue (Avertir et continuer) en fonction des paramètres d'évaluation du contenu du site dans le groupe de politiques d'accès. La demande du client visait du contenu pour adultes et la politique est configurée pour envoyer un avertissement aux utilisateurs qui accèdent à un contenu pour adultes.
BLOCK_CONTINUE_CUSTOMCAT	Transaction bloquée et affichage de la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL personnalisée dans le groupe de politiques d'accès configurée sur « Warn » (Avertir).
BLOCK_CONTINUE_WEBCAT	Transaction bloquée et affichage de la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir).
BLOCK_CUSTOMCAT	Transaction bloquée en fonction des paramètres de filtrage de catégorie d'URL personnalisée pour le groupe de politiques d'accès.
BLOCK_ICAP	Le proxy Web a bloqué la demande en fonction du verdict du système DLP externe comme défini dans le groupe de politiques DLP externe.
BLOCK_SEARCH_UNSAFE	La demande du client incluait une requête de recherche non sécurisée et la politique d'accès est configurée pour appliquer des recherches sécurisées, de sorte que la demande initiale du client a été bloquée.
BLOCK_SUSPECT_USER_AGENT	Transaction bloquée en fonction du paramètre Suspect User Agent (Agent utilisateur suspect) pour le groupe de politiques d'accès.
BLOCK_UNSUPPORTED_SEARCH_APP	Transaction bloquée en fonction des paramètres de recherche sécurisée pour le groupe de politiques d'accès. La transaction visait un moteur de recherche non pris en charge, et la politique est configurée pour bloquer les moteurs de recherche non pris en charge.
BLOCK_WBRS	Transaction bloquée en fonction des paramètres de filtre de réputation Web pour le groupe de politiques d'accès.
BLOCK_WBRS_IDS	Le proxy Web a bloqué la demande de chargement en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de sécurité des données.

Balise de décision ACL	Description
BLOCK_WEBCAT	Transaction bloquée en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de politiques d'accès.
BLOCK_WEBCAT_IDS	Le proxy Web a bloqué la demande de chargement en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de politiques de sécurité des données.
BLOCK_YTCAT	Le proxy Web a bloqué la transaction en fonction des paramètres de filtrage de catégories YouTube prédéfinis pour le groupe de politiques d'accès.
BLOCK_CONTINUE_YTCAT	Le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie YouTube prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir).
DECRYPT_ADMIN	Le proxy Web a déchiffré la transaction en fonction de certains paramètres par défaut pour le groupe de politiques de déchiffrement.
DECRYPT_ADMIN_EXPIRED_CERT	Le proxy Web a déchiffré la transaction bien que le certificat du serveur ait expiré.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	Le proxy Web a déchiffré la transaction en fonction des paramètres par défaut comme l'abandon de connexion pour le groupe de politiques de déchiffrement quand EUN est activé.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS ont abandonné un certificat expiré avec EUN activé.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS ont abandonné un certificat feuille non valide avec EUN activé.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS suppriment le nom d'hôte non concordant avec EUN activé.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS abandonnent un OCSP avec d'autres erreurs avec EUN activé.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS ont abandonné un certificat OCSP révoqué avec EUN activé.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS abandonnent un certificat d'autorité racine ou d'émetteur non reconnu avec EUN activé.
DECRYPT_EUN_CUSTOMCAT	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégories d'URL personnalisées pour le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.

Balise de décision ACL	Description
DECRYPT_EUN_WBRS	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.
DECRYPT_EUN_WBRS_NO_SCORE	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web pour les URL sans score de réputation dans le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.
DECRYPT_EUN_WEBCAT	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégories d'URL pour le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.
DECRYPT_WEBCAT	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de politiques de déchiffrement.
DECRYPT_WBRS	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement.
DEFAULT_CASE	Le proxy Web a permis au client d'accéder au serveur, car aucun des services AsyncOS, tels que la réputation de sites Web ou l'analyse de protection contre les programmes malveillants , n'a pris de mesures sur la transaction.
DENY_ADMIN	Le proxy Web a refusé la transaction. Cela se produit pour les demandes HTTPS lorsque l'authentification est requise et que l'option « Decrypt for Authentication » (Déchiffrer pour authentification) est désactivée dans les paramètres de proxy HTTPS.
DROP_ADMIN	Le proxy Web a abandonné la transaction en fonction de certains paramètres par défaut pour le groupe de politiques de déchiffrement.
DROP_ADMIN_EXPIRED_CERT	Le proxy Web a abandonné la transaction, car le certificat du serveur a expiré.
DROP_WEBCAT	Le proxy Web a abandonné la transaction en fonction des paramètres de filtrage de catégories d'URL pour le groupe de politiques de déchiffrement.
DROP_WBRS	Le proxy Web a abandonné la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement.
MONITOR_ADC	Le proxy Web a surveillé la transaction en fonction des paramètres d'application pour le groupe de politiques d'accès.
MONITOR_ADMIN_EXPIRED_CERT	Le proxy Web a surveillé la réponse du serveur, car le certificat du serveur a expiré.

Balise de décision ACL	Description
MONITOR_AMP_RESP	Le proxy Web a surveillé la réponse du serveur en fonction des paramètres Cisco Secure Endpoint du groupe de politiques d'accès.
MONITOR_AMW_RESP	Le proxy Web a surveillé la réponse du serveur en fonction des paramètres contre les programmes malveillants pour le groupe des politiques d'accès.
MONITOR_AMW_RESP_URL	Le proxy Web soupçonne que l'URL contenue dans la demande HTTP n'est pas sûre, mais il a surveillé la transaction en fonction des paramètres contre les programmes malveillants pour le groupe des politiques d'accès.
MONITOR_AVC	Le proxy Web a surveillé la transaction en fonction des paramètres d'application pour le groupe de politiques d'accès.
MONITOR_CONTINUE_CONTENT_ UNSAFE	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction des paramètres d'évaluation du contenu du site dans le groupe de politiques d'accès. La demande du client visait du contenu pour adultes et la politique est configurée pour envoyer un avertissement aux utilisateurs qui accèdent à un contenu pour adultes. L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_CONTINUE_CUSTOMCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL personnalisée dans le groupe de politiques d'accès configuré sur « Warn » (Avertir). L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_CONTINUE_WEBCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir). L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_CONTINUE_YTCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie YouTube prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir). L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_IDS	Le proxy Web a analysé la demande de chargement à l'aide d'une politique de sécurité des données ou d'une politique DLP externe, mais n'a pas bloqué la demande. Il a évalué la demande par rapport aux politiques d'accès.

Balise de décision ACL	Description
MONITOR_SUSPECT_USER_AGENT	Le proxy Web a surveillé la transaction en fonction du paramètre Suspect User Agent (Agent utilisateur suspect) pour le groupe de politiques d'accès.
MONITOR_WBRS	Le proxy Web a surveillé la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques d'accès.
NO_AUTHORIZATION	Le proxy Web n'a pas autorisé l'utilisateur à accéder à l'application, car l'utilisateur était déjà authentifié par rapport à un domaine d'authentification, mais pas par rapport à un domaine d'authentification configuré dans la politique d'authentification de l'application.
NO_PASSWORD	L'authentification de l'utilisateur a échoué.
PASSTHRU_ADMIN	Le proxy Web a transmis la transaction en fonction de certains paramètres par défaut pour le groupe de politiques de déchiffrement.
PASSTHRU_ADMIN_EXPIRED_CERT	Le proxy Web a effectué la transaction bien que le certificat du serveur ait expiré.
PASSTHRU_WEBCAT	Le proxy Web a transmis la transaction en fonction des paramètres de filtrage de catégories d'URL pour le groupe de politiques de déchiffrement.
PASSTHRU_WBRS	Le proxy Web a transmis la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement.
REDIRECT_CUSTOMCAT	Le proxy Web a redirigé la transaction vers une URL différente en fonction d'une catégorie d'URL personnalisée dans le groupe de politiques d'accès configuré sur « Redirect » (Rediriger).
SAAS_AUTH	Le proxy Web a autorisé l'utilisateur à accéder à l'application, car l'utilisateur a été authentifié de manière transparente par rapport au domaine d'authentification configuré dans la politique d'authentification de l'application.
OTHER	Le proxy Web n'a pas traité la demande en raison d'une erreur, comme un échec d'autorisation, la déconnexion du serveur ou une abandon par le client.

Interprétation des entrées de verdict d'analyse des journaux d'accès

Les entrées du fichier journal des accès regroupent et affichent les résultats des différents moteurs d'analyse, tels que le filtrage d'URL, le filtrage de réputation Web et l'analyse contre les programmes malveillants. L'appliance affiche ces informations entre crochets en angle à la fin de chaque entrée du journal d'accès.

Le texte qui suit constitue le verdict d'analyse provenant d'une entrée de fichier journal des accès. Dans cet exemple, le moteur d'analyse Webroot a détecté le programme malveillant :

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",
-,-,
IW_infr,-,"Trojan Phisher","-","-","Unknown","Unknown","-","-",489.73,0,

[Local],"-","-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf",

"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e",

ARCHIVESCAN_BLOCKEDFILETYPE,

EXT_ARCHIVESCAN_VERDICT,

EXT_ARCHIVESCAN_THREATDETAIL,

EXT_WTT_BEHAVIOR,
EXT_YTCAT,
"BlockedFileType: application/x-rpm,
BlockedFile: allfiles/linuxpackage.rp">
```

Note Pour obtenir un exemple d'entrée complète de fichier journal des accès, consultez Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500.

Chaque élément dans cet exemple correspond à un spécificateur de format de fichier journal, comme le montre le tableau suivant :

Position	Valeur de champ	Spécificateur de format	Description
1	`IW_infr`	%XC	La catégorie d'URL personnalisée attribuée à la transaction, en abrégé. Ce champ affiche « nc » lorsqu'aucune catégorie n'est attribuée.
2	`ns`	%XW	Score des filtres de réputation Web Ce champ affiche le score, sous forme de nombre, « ns » pour aucun score ou « dns » en cas d'erreur de recherche DNS.
3	`24`	%Xv	Le verdict d'analyse des programmes malveillants Webroot est transmis au moteur DVS. S'applique aux réponses détectées par Webroot uniquement. Pour en savoir plus, consultez Valeurs de verdict de la recherche de programmes malveillants, on page 543.
4	`"Trojan-Phisher-Gamec"`	"%Xn"	Nom du logiciel espion associé à l'objet. S'applique aux réponses détectées par Webroot uniquement.
5	`0`	%Xt	Valeur spécifique à Webroot associée à la valeur du rapport menaces/risques (TRR) qui détermine la probabilité qu'un programme malveillant existe. S'applique aux réponses détectées par Webroot uniquement.

Position	Valeur de champ	Spécificateur de format	Description
6	`354385`	%Xs	Valeur que Webroot utilise comme identifiant de menace. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par Webroot uniquement.
7	`12559`	%Xi	Valeur que Webroot utilise comme ID Trace. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par Webroot uniquement.
8	-	%Xd	Le verdict d'analyse contre les programmes malveillants que McAfee a transmis au moteur DVS. S'applique aux réponses détectées par McAfee uniquement. Pour en savoir plus, consultez Valeurs de verdict de la recherche de programmes malveillants, on page 543.
9	"-"	"%Xe"	Nom du fichier analysé par McAfee. S'applique aux réponses détectées par McAfee uniquement.
10	-	%Xf	Valeur que McAfee utilise comme erreur d'analyse. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par McAfee uniquement.
11	-	%Xg	Valeur que McAfee utilise comme type de détection. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par McAfee uniquement.
12	-	%Xh	Valeur que McAfee utilise comme type de virus. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par McAfee uniquement.
13	"-"	"%Xj"	Le nom du virus que McAfee a analysé. S'applique aux réponses détectées par McAfee uniquement.

Position	Valeur de champ	Spécificateur de format	Description
14	-	%XY	Le verdict de l'analyse contre les programmes malveillants Sophos a transmis au moteur DVS. S'applique uniquement aux réponses détectées par Sophos. Pour en savoir plus, consultez Valeurs de verdict de la recherche de programmes malveillants, on page 543.
15	-	%Xx	Une valeur que Sophos utilise comme code de retour d'analyse. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique uniquement aux réponses détectées par Sophos.
16	"-"	"%Xy"	Nom du fichier dans lequel Sophos a trouvé le contenu répréhensible. S'applique uniquement aux réponses détectées par Sophos.
17	"-"	"%Xz"	Une valeur que Sophos utilise comme nom de menace. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique uniquement aux réponses détectées par Sophos.
18	-	%Xl	Le verdict de l'analyse sur la sécurité des données de Cisco en fonction de l'action dans la colonne Contenu de la politique de sécurité des données de Cisco. La liste suivante décrit les valeurs possibles pour ce champ : • **0.** Allow (Autoriser) • **1.** Block (Bloquer) • **- (trait d'union).** Aucune analyse n'a été lancée par les filtres de sécurité des données Cisco. Cette valeur s'affiche lorsque les filtres de sécurité des données Cisco sont désactivés ou lorsque l'action de catégorie d'URL est définie sur Allow (autoriser).

Position	Valeur de champ	Spécificateur de format	Description
19	-	%Xp	Verdict de l'analyse DLP externe en fonction du résultat donné dans la réponse ICAP . La liste suivante décrit les valeurs possibles pour ce champ : • **0.** Allow (Autoriser) • **1.** Block (Bloquer) • **- (trait d'union).** Aucune analyse n'a été lancée par le serveur DLP externe. Cette valeur s'affiche lorsque l'analyse DLP externe est désactivée ou lorsque le contenu n'a pas été analysé en raison d'une catégorie d'URL dispensée dans la page External DLP Policies > Destinations (Politiques DLP externes > Destinations).
20	`IW_infr`	%XQ	Verdict de catégorie d'URL prédéfinie déterminé lors de l'analyse côté demande, en abrégé. Ce champ répertorie un tiret (-) lorsque le filtrage d'URL est désactivé. **Note** Dans AsyncOS version 11.8 et ultérieure, l'identifiant de catégorie d'URL apparaît entre guillemets doubles. Par exemple, « IW_infr ». Pour obtenir la liste des abréviations de catégories d'URL, consultez Descriptions des catégories d'URL, on page 228.
21	-	%XA	Verdict de la catégorie d'URL déterminé par le moteur d'analyse de contenu dynamique lors de l'analyse du côté des réponses, en abrégé. S'applique uniquement au moteur de filtrage d'URL Cisco Web Usage Controls. S'applique uniquement lorsque le moteur d'analyse de contenu dynamique est activé et lorsqu'aucune catégorie n'est attribuée au moment de la demande (une valeur « nc » est indiquée dans le verdict de l'analyse du côté de la demande). Pour obtenir la liste des abréviations de catégories d'URL, consultez Descriptions des catégories d'URL, on page 228.

Position	Valeur de champ	Spécificateur de format	Description
22	"Trojan Phisher"	"%XZ"	Verdict unifié de l'analyse contre les programmes malveillants côté réponse qui fournit la catégorie de programmes malveillants indépendamment des moteurs d'analyse sont activés. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur.
23	"-"	"%Xk"	Le nom de la catégorie ou le type de menace est renvoyé par les filtres de réputation Web. Le nom de la catégorie est renvoyé lorsque la réputation Web est élevée et le type de menace est renvoyé lorsque la réputation est faible.
24	"-"	%X#10#	URL qui est encapsulée dans le moteur de traduction Google. S'il n'y a pas d'URL encapsulée, la valeur du champ sera « - ».
25	"Unknown"	"%XO"	Le nom de l'application tel qu'il a été renvoyé par le moteur AVC, le cas échéant. Ne s'applique que lorsque le moteur AVC est activé.
26	"Unknown"	"%Xu"	Le type d'application tel qu'il est renvoyé par le moteur AVC, le cas échéant. Ne s'applique que lorsque le moteur AVC est activé.
27	"-"	"%Xb"	Le comportement de l'application tel qu'il est renvoyé par le moteur AVC, le cas échéant. Ne s'applique que lorsque le moteur AVC est activé.
28	"-"	"%XS"	Verdict de l'analyse pour une navigation sécurisée Cette valeur indique si la fonction de recherche sécurisée ou d'évaluation du contenu du site a été appliquée à la transaction. Pour obtenir la liste des valeurs possibles, consultez Journalisation de l'accès au contenu pour adultes, on page 220.
29	489.73	%XB	La bande passante moyenne utilisée pour servir la demande, en Ko/s.
30	0	%XT	Valeur qui indique si la demande a été limitée en raison des paramètres de contrôle de limite de bande passante, où « 1 » indique que la demande a été limitée et « 0 » le contraire.

Position	Valeur de champ	Spécificateur de format	Description
31	`[Local]`	%l	Le type d'utilisateur effectuant la demande, « [Local] » ou « [Remote] ». Ne s'applique que lorsqu'AnyConnect Secure Mobility est activé. Lorsqu'elle n'est pas activée, la valeur est un tiret (-).
32	`"-"`	"%X3"	Verdict unifié de l'analyse contre les programmes malveillants du côté de la demande, quel que soit le moteur d'analyse activé. S'applique aux transactions bloquées ou surveillées en raison de l'analyse des demandes des clients lorsqu'une politique d'analyse des programmes malveillants sortants s'applique.
33	`"-"`	"%X4"	Le nom de menace attribué à la demande du client qui a été bloquée ou surveillée en raison d'une politique d'analyse de programmes malveillants sortants applicable. Ce nom de menace est indépendant des moteurs d'analyse activés de protection contre les programmes malveillants.
34	`37`	%X#1#	Verdict de l'analyse des fichiers Cisco Secure Endpoint : • 0 : le fichier n'est pas malveillant • 1 : Le fichier n'a pas été analysé en raison de son type de fichier • 2 : L'analyse des fichiers a expiré • 3 : Erreur d'analyse • Supérieur à 3 : Le fichier est malveillant
35	`"W32.CiscoTestVector"`	%X#2#	Le nom de la menace, comme déterminé par l'analyse de fichiers Cisco Secure Endpoint; « - » indique l'absence de menace.

Position	Valeur de champ	Spécificateur de format	Description
36	`33`	%X#3#	Score de réputation résultant de l'analyse des fichiers Cisco Secure Endpoint. Ce score est utilisé uniquement si le service de réputation en nuage n'est pas en mesure de déterminer un verdict clair pour le fichier. Pour en savoir plus, consultez les informations sur le score de menaces et le seuil de réputation dans Filtrage de réputation de fichiers et analyse de fichiers, on page 323. .
37	`0`	%X#4#	Indicateur de chargement et de demande d'analyse : « 0 » indique que Cisco Secure Endpoint n'a pas demandé le chargement du fichier pour analyse. « 1 » indique que Cisco Secure Endpoint a demandé le chargement du fichier pour analyse.
38	`"WSA-INFECTED-FILE.pdf"`	%X#5#	Nom du fichier en cours de téléchargement et d'analyse.
39	`"fd5ef49d4213e05f448 f11ed9c98253d85829614fba 368a421d14e64c426da5e"`	%X#6#	Identifiant SHA-256 de ce fichier.
40	`ARCHIVESCAN_BLOCKEDFILETYPE`	%X#8#	Verdict de l'analyse des archives
41	`EXT_ARCHIVESCAN_VERDICT`	%Xo	Détails du verdict d'analyse d'archives. Si un fichier d'archive pouvant être inspectée est bloqué (`ARCHIVESCAN_BLOCKEDFILETYPE`) en fonction des paramètres de la politique d'accès : blocage des objets personnalisés, cette entrée de détail du verdict inclut le type de fichier bloqué et le nom du fichier bloqué.
42	`EXT_ARCHIVESCAN_THREATDETAIL`	%Xm	Fichier verdict par l'analyseur d'archives
43	`EXT_WTT_BEHAVIOR`	%XU	Comportement de dérivation Web.
44	`EXT_YTCAT`	%X#29#	La catégorie d'URL YouTube attribuée à la transaction, en abrégé. Ce champ affiche « nc » lorsqu'aucune catégorie n'est attribuée.

Reportez-vous à la section Champs et balises des fichiers journaux, on page 528 pour obtenir une description de la fonction de chaque spécificateur de format.

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500
- Personnalisation des journaux d'accès, on page 523
- Fichiers journaux des accès conformes aux normes W3C, on page 521
- Affichage des fichiers journaux, on page 499
- Champs et balises des fichiers journaux, on page 528

Fichiers journaux des accès conformes aux normes W3C

Secure Web Appliance fournit deux types de journaux différents pour l'enregistrement des informations sur les transactions par proxy Web : les journaux d'accès et les journaux d'accès au format W3C. Les journaux d'accès W3C sont conformes à la norme World Wide Web Consortium (W3C) et enregistrent l'historique des transactions dans le format ELF (Extended Log File) du W3C.

- Types de champs W3C, on page 521
- Interprétation des journaux d'accès W3C, on page 521

Types de champs W3C

Lors de la définition d'un abonnement au journal des accès W3C, vous devez choisir les champs de journalisation à inclure, comme la balise de décision ACL ou l'adresse IP du client. Vous pouvez inclure l'un des types de champs de journal suivants :

- **Prédéfini.** L'interface Web comprend une liste de champs parmi lesquels vous pouvez choisir.
- **Défini par l'utilisateur.** Vous pouvez saisir un champ de journal qui ne figure pas dans la liste prédéfinie.

Interprétation des journaux d'accès W3C

Tenez compte des règles et des directives suivantes lors de l'interprétation des journaux d'accès W3C :

- Les administrateurs décident quelles données sont enregistrées dans chaque abonnement au journal des accès W3C; par conséquent, les journaux d'accès W3C n'ont pas de format de champ défini.
- Les journaux W3C sont autodescriptifs. Le format de fichier (liste des champs) est défini dans un en-tête au début de chaque fichier journal.
- Les champs des journaux d'accès W3C sont séparés par un espace.
- Si un champ ne contient aucune donnée pour une entrée en particulier, un tiret (-) est inclus dans le fichier journal.
- Chaque ligne du fichier journal des accès W3C est liée à une transaction et chaque ligne se termine par une séquence LF.

- En-têtes des fichiers journaux W3C, on page 522
- Préfixes des champs W3C, on page 522

En-têtes des fichiers journaux W3C

Chaque fichier journal W3C contient un texte d'en-tête au début du fichier. Chaque ligne commence par le caractère # et fournit des renseignements sur Secure Web Appliance qui a créé le fichier journal. Les en-têtes du fichier journal W3C comprennent également le format de fichier (liste des champs), ce qui rend le fichier journal autodescriptif.

Le tableau suivant décrit les champs d'en-tête répertoriés au début de chaque fichier journal W3C.

Champ d'en-tête	Description
Version	Version du format ELF W3C utilisée.
Date	Date et heure auxquelles l'en-tête (et le fichier journal) a été créé.
System (Système)	Secure Web Appliance qui a généré le fichier journal au format « Management_IP - Management_hostname ».
Software (Logiciel)	Logiciel qui a généré ces journaux
Fields (Champs)	Champs enregistrés dans le journal

Exemple de fichier journal W3C :

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
#Software: AsyncOS for Web 6.3.0
#Fields: timestamp x-elapsed-time c-ip
x-resultcode-httpstatus sc-bytes cs-method cs-url cs-username
x-hierarchy-origin cs-mime-type x-acltag x-result-code x-suspect-user-agent
```

Préfixes des champs W3C

La plupart des noms de champs des journaux W3C comprennent un préfixe qui identifie l'en-tête dont provient une valeur, comme le client ou le serveur. Les champs de journalisation sans préfixe référencent des valeurs indépendantes des ordinateurs impliqués dans la transaction. Le tableau suivant décrit les préfixes des champs des journaux W3C.

En-tête de préfixe	Description
c	Client
s	Serveur
cs	Client vers serveur
sc	Serveur vers client
x	Identifiant spécifique à l'application.

Par exemple, le champ de journal W3C « cs-method » fait référence à la méthode dans la demande envoyée par le client au serveur et « c-ip » fait référence à l'adresse IP du client.

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500.
- Personnalisation des journaux d'accès, on page 523.
- Fichiers journaux de supervision du trafic, on page 528.
- Champs et balises des fichiers journaux, on page 528.
- Affichage des fichiers journaux, on page 499.

Personnalisation des journaux d'accès

Vous pouvez personnaliser les journaux d'accès standard et W3C pour inclure de nombreux champs différents afin de saisir des informations complètes sur le trafic Web au sein du réseau à l'aide de champs prédéfinis ou définis par l'utilisateur.

Thèmes connexes

- Pour obtenir la liste des champs prédéfinis, consultez Champs et balises des fichiers journaux, on page 528.
- Pour en savoir plus sur les champs définis par l'utilisateur, consultez Champs définis par l'utilisateur des journaux d'accès, on page 523.

Champs définis par l'utilisateur des journaux d'accès

Si la liste des champs prédéfinis de journal d'accès et de journal W3C n'inclut pas toutes les informations d'en-tête que vous souhaitez enregistrer à partir des transactions HTTP/HTTPS, vous pouvez taper un champ de journal défini par l'utilisateur dans la zone de texte Champs personnalisés lorsque vous configurez l'accès et le journal W3C.

Les champs de journal personnalisés peuvent comprendre n'importe quelle donnée de n'importe quel en-tête envoyé par le client ou le serveur. Si une demande ou une réponse ne comprend pas l'en-tête ajouté à l'abonnement au journal, le fichier journal comprend un tiret comme valeur de champ de journal.

Le tableau suivant définit la syntaxe à utiliser pour l'accès et les journaux W3C :

Type d'en-tête	Syntaxe du spécificateur de format du journal d'accès	Syntaxe du champ personnalisé du journal W3C
En-tête de l'application cliente	%<*ClientHeaderName* :	cs(*ClientHeaderName*)
En-tête du serveur	%<*ServerHeaderName* :	sc(*ServerHeaderName*)

Par exemple, si vous souhaitez consigner la valeur d'en-tête If-Modified-Since dans les demandes des clients, entrez le texte suivant dans la zone Custom Fields (Champs personnalisés) pour un abonnement de journal W3C :

```
cs(If-Modified-Since)
```

Thèmes connexes

- Personnalisation des journaux d'accès standard, on page 524.
- Personnalisation des journaux d'accès W3C, on page 524.

Personnalisation des journaux d'accès standard

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur le nom du fichier journal des accès pour modifier l'abonnement au journal des accès.

Étape 3 Entrez les spécificateurs de format requis dans le champ personnalisé.

La syntaxe de saisie des spécificateurs de format dans le champ personnalisé est la suivante :

```
<format_specifier_1> <format_specifier_2> ...
```

Par exemple : `%a %b %E`

Vous pouvez ajouter des jetons avant les spécificateurs de format pour afficher un texte de description dans le fichier journal des accès. Par exemple :

```
client_IP %a body_bytes %b error_type %E
```

où `IP_client` est le jeton de description du spécificateur de format de journal `%a`, etc.

Note Vous pouvez créer un champ personnalisé pour tout en-tête dans une demande de client ou une réponse de serveur.

Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500.
- Champs et balises des fichiers journaux, on page 528.
- Champs définis par l'utilisateur des journaux d'accès, on page 523.

Personnalisation des journaux d'accès W3C

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur le nom du fichier journal W3C pour modifier l'abonnement au journal W3C.

Étape 3 Saisissez un champ dans la zone Custom Field (Champ personnalisé), puis cliquez sur **Add** (Ajouter).

L'ordre dans lequel les champs apparaissent dans la liste Selected Log Fields (Champs de journal sélectionnés) détermine l'ordre des champs dans le fichier du journal d'accès W3C. Vous pouvez modifier l'ordre des champs à l'aide des boutons **Déplacement vers le haut** et **Déplacement vers le bas**. Vous pouvez supprimer un champ en le sélectionnant dans la liste Selected Log Fields (Champs de journal sélectionnés) et en cliquant sur **Remove** (Supprimer).

Vous pouvez saisir plusieurs champs définis par l'utilisateur dans la zone Custom Fields (Champs personnalisés) et les ajouter simultanément à condition que chaque entrée soit séparée par une nouvelle ligne [cliquez sur Enter (Entrée)] avant de cliquer sur **Add** (Ajouter).

Lorsque vous modifiez les champs de journal inclus dans un abonnement à un journal W3C, l'abonnement au journal est automatiquement renouvelé. Cela permet à la dernière version du fichier journal d'inclure les nouveaux en-têtes de champ corrects

Note Vous pouvez créer un champ personnalisé pour tout en-tête dans une demande de client ou une réponse de serveur.

Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Fichiers journaux des accès conformes aux normes W3C, on page 521.
- Champs et balises des fichiers journaux, on page 528.
- Champs définis par l'utilisateur des journaux d'accès, on page 523.
- Configuration des journaux W3C personnalisés propres à Cisco CTA, on page 525
- Configuration des journaux W3C personnalisés propres à Cisco Cloudlock, on page 526

Configuration des journaux W3C personnalisés propres à Cisco CTA

Vous pouvez configurer votre appliance pour transmettre les journaux d'accès W3C propres à Cognitive Threat Analytics (CTA) au service Cisco Cloud Web Security à des fins d'analyse et de création de rapports. Cisco ScanCenter est le portail d'administration de Cloud Web Security (CWS). Voir la section https://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html.

Avant de commencer

Créez un compte de périphérique dans Cisco ScanCenter pour votre appliance en sélectionnant SCP (Secure Copy Protocol) comme protocole de téléchargement automatique. Voir la section des téléchargements de périphériques de proxy dans le logiciel Cisco ScanCenter Administrator (https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide.html).

Notez le nom d'hôte SCP et le nom d'utilisateur généré pour votre appliance. Le nom d'utilisateur est sensible à la casse et unique pour chaque périphérique.

Étape 1 Choisissez **Security Services** > **Cisco Cognitive Threat Analytics** (Services de sécurité > Cisco Cognitive Threat Analytics).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la zone **Log Fields** (Champs de journal), ajoutez des champs de journal supplémentaires, au besoin. Consultez Ajout et modification d'abonnements aux journaux, à la page 491.

Étape 4 Dans **Selected Log Fields** (Champs de journal sélectionnés), cochez les cases en regard de *c-ip*, *cs-username* ou *cs-auth-group* si vous souhaitez anonymiser ces champs individuellement.

Vous pouvez également cocher la case **Anonymization** (Anonymisation) pour anonymiser ces champs simultanément. Consultez Ajout et modification d'abonnements aux journaux, à la page 491.

Étape 5 Dans la zone **Rerieval Method** (Méthode de récupération), saisissez le nom d'utilisateur généré pour votre périphérique dans Cisco ScanCenter. Le nom d'utilisateur du périphérique est sensible à la casse et unique pour chaque périphérique proxy.

Étape 6 Modifiez les valeurs dans **Advanced Options** (Options avancées), si nécessaire.

Étape 7 Cliquez sur **Submit** (Soumettre).

L'appliance génère des clés SSH publiques et les affiche sur la page Cisco Cognitive Threat Analytics.

Étape 8 Copiez une des clés SSH publiques dans le presse-papiers.

Étape 9 Cliquez sur le lien du portail **Cisco Cognitive Threat Analytics** pour basculer vers le portail Cisco ScanCenter, sélectionnez le compte de périphérique approprié, puis collez la clé SSH publique dans la page de provisionnement de l'appareil CTA. (Reportez-vous à la section sur les *chargements de périphériques proxy* du Guide de l'administrateur de Cisco ScanCenter.)

Les fichiers journaux de votre périphérique proxy seront chargés sur le système CTA pour une analyse de l'authentification réussie entre votre périphérique proxy et le système CTA.

Étape 10 Revenez à l'appliance et validez vos modifications.

Vous pouvez également ajouter des journaux CTA W3C en utilisant **System Administration** > **Log Subscription** (Administration système > Abonnement aux journaux). Suivez les instructions à la section Personnalisation des journaux d'accès W3C, à la page 524 pour ajouter un nouvel abonnement au journal des accès W3C avec les options suivantes :

- **Journaux W3C** comme type de journal
- **Cisco Cognitive Threat Analytics Subscription** en tant qu'abonnement
- **SCP** comme type de transfert de fichier

Consultez Ajout et modification d'abonnements aux journaux, à la page 491 pour en savoir plus sur les champs personnalisés.

Remarque Si vous avez déjà configuré un abonnement à la journalisation CTA, vous devez remplacer le nom du journal par *cta_log* pour l'afficher sur la page Cisco Cognitive Threat Analytics de l'appliance.

Après la création du journal, si vous souhaitez supprimer le journal CTA, cliquez sur **Disable** (Désactiver) dans la page Cisco Cognitive Threat Analytics. Vous pouvez également supprimer le journal CTA de la page des abonnements aux journaux [**System Administration** > **Log subscriptions** (Administration système > Abonnements aux journées)].

Cliquez sur **Deanonymize** (Désanonymiser) dans la page Cisco Cognitive Threat Analytics de Cisco Cognitive Threat Analytics pour désanonymiser les champs du journal W3C spécifiques au CTA. Voir la section Désanonymisation des champs de journalisation W3C, à la page 496.

Vous pouvez également désanonymiser les champs de journalisation anonymisés propres au CTA du W3C en utilisant **System Administration** > **Log Subscription** (Administration système > Abonnement aux journaux). Voir la section Désanonymisation des champs de journalisation W3C, à la page 496.

Configuration des journaux W3C personnalisés propres à Cisco Cloudlock

Cisco Cloudlock est une plateforme infonuagique du CASB et de cybersécurité en nuage qui protège les utilisateurs, les données et les applications sur les logiciels-services, les plateformes en tant que service et les infrastructures en tant que service. Vous pouvez configurer votre appliance pour pousser les journaux d'accès W3C vers le portail Cisco Cloudlock à des fins d'analyse et de création de rapports. Ces journaux W3C personnalisés offrent une meilleure visibilité sur l'utilisation des logiciels-services par les clients.

Avant de commencer

Créez un compte de périphérique dans le portail Cloudlock pour votre appliance en sélectionnant SCP comme protocole de téléchargement automatique.

Connectez-vous au portail Cloudlock, accédez à l'aide en ligne et suivez les instructions pour créer un compte de périphérique sur le portail Cloudlock.

Étape 1 Choisissez **Security Services** > **Cisco Cloudlock** (Services de sécurité > Cisco Cloudlock).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Remarque Les champs de journalisation sont sélectionnés par défaut dans la zone **Log Fields** (Champs de journal). Vous ne pouvez pas ajouter d'autres champs de journalisation que les champs de journalisation sélectionnés par défaut. Vous ne devez pas modifier l'ordre des champs du journal affichés dans la zone **Log Fields** (Champs de journal).

Vous ne pouvez pas anonymiser les champs (*c-ip, cs-username* ou *cs-auth-group*) des fichiers journaux Cloudlock.

Étape 3 Dans la zone **Retrieval Method** (Méthode de récupération), entrez les informations suivantes :

- Nom d'hôte et numéro de port du serveur Cloudlock
- Répertoire sur le serveur Cloudlock pour stocker le fichier journal
- Nom de l'utilisateur autorisé à se connecter au serveur Cloudlock

Étape 4 Modifiez les valeurs dans **Advanced Options** (Options avancées), si nécessaire.

Étape 5 Cliquez sur **Submit** (Soumettre).

L'appliance génère des clés SSH publiques et les affiche sur la page Cisco Cloudlock.

Étape 6 Copiez une des clés SSH publiques dans le presse-papiers.

Étape 7 Cliquez sur le lien **View Cloudlock Portal** (Afficher le portail Cisco Cloudlock) pour passer au portail Cisco Cloudlock. Sélectionnez le compte de périphérique approprié, puis collez la clé SSH publique dans la page des paramètres Cloudlock.

Les fichiers journaux de votre périphérique proxy seront téléchargés sur le système Cloudlock pour une analyse de l'authentification réussie entre votre périphérique proxy et le système Cloudlock.

Étape 8 Revenez à l'appliance et validez vos modifications.

Vous pouvez également ajouter des journaux Cloudlock W3C en sélectionnant **System Administration** > **Log Subscription** (Administration système > Abonnement aux journaux). Suivez les instructions à la section Personnalisation des journaux d'accès W3C, à la page 524 pour ajouter un nouvel abonnement au journal des accès W3C avec les options suivantes :

- **Journaux W3C** comme type de journal
- **Cisco Cloudlock** en tant qu'abonnement
- **SCP** comme type de transfert de fichier

Consultez Ajout et modification d'abonnements aux journaux, à la page 491 pour en savoir plus sur les champs personnalisés.

Remarque Si vous avez déjà configuré un abonnement à la journalisation Cloudlock, vous devez remplacer le nom du journal par **cloudlock_log** pour l'afficher sur la page Cisco Cloudlock de l'appliance.

Après la création du journal, si vous souhaitez supprimer le journal Cloudlock, cliquez sur **Disable** (Désactiver) dans la page Cisco Cloudlock. Vous pouvez également supprimer le journal Cloudlock à partir de la page des abonnements aux journaux [**System Administration** > **Log subscriptions** (Administration système > Abonnements aux journaux)].

Fichiers journaux de supervision du trafic

Les fichiers journaux de la supervision du trafic de la couche 4 fournissent un enregistrement détaillé de l'activité de supervision sur la couche 4. Vous pouvez afficher les entrées de fichier journal de la supervision du trafic de la couche 4 pour suivre les mises à jour des listes de blocage et des listes d'autorisation de pare-feu.

Interprétation des journaux de supervision du trafic

Utilisez les exemples ci-dessous pour interpréter les différents types d'entrées contenues dans les journaux de supervision du trafic.

Exemple 1

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) ajouté à la liste de blocage du pare-feu.
```

Dans cet exemple, où une correspondance devient une entrée de pare-feu de liste de blocage. La supervision du trafic de la couche 4 a mis en correspondance une adresse IP et un nom de domaine dans la liste de blocage en fonction d'une demande DNS qui est passée par l'appliance. L'adresse IP est ensuite entrée dans la liste de blocage du pare-feu.

Exemple 2

```
172.xx.xx.xx découvert pour www.allowsite.com (www.allowsite.com) ajouté à la liste des autorisations du pare-feu.
```

Dans cet exemple, une correspondance devient une entrée de pare-feu de liste d'autorisation. La supervision du trafic de la couche 4 a trouvé une entrée de nom de domaine et l'a ajoutée à la liste des autorisations de l'appliance. L'adresse IP est ensuite entrée dans la liste d'autorisation du pare-feu.

Exemple 3

```
Le pare-feu a noté les données de 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

Dans cet exemple, la supervision du trafic de la couche 4 consigne un enregistrement des données transmises entre une adresse IP interne et une adresse IP externe qui se trouve sur la liste de blocage. De plus, la supervision du trafic de la couche 4 est configurée pour surveiller, pas pour bloquer.

Thèmes connexes

- Affichage des fichiers journaux, on page 499

Champs et balises des fichiers journaux

- Spécificateurs de format des journaux d'accès et champs des fichiers journaux W3C, on page 529

• Codes de résultats de transactions, on page 504
• Balises de décision ACL, on page 505
• Valeurs de verdict de la recherche de programmes malveillants, on page 543

Spécificateurs de format des journaux d'accès et champs des fichiers journaux W3C

Les fichiers journaux utilisent des variables pour représenter les éléments d'information qui composent chaque entrée de fichier journal. Ces variables sont appelées spécificateurs de format dans les journaux d'accès et champs de journalisation dans les journaux W3C. Chaque spécificateur de format est associé à un champ de journal.

Pour configurer les journaux d'accès afin d'afficher ces valeurs, consultez Personnalisation des journaux d'accès, on page 523 et les informations sur les champs personnalisés dans Ajout et modification d'abonnements aux journaux, on page 491.

Le tableau suivant décrit ces variables :

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%:<A	AclTime	Pour imprimer le temps total nécessaire à la transaction de liste de contrôle d'accès.
%{	x-id-shared	Pour imprimer l'état du partage d'ID avec Cisco Umbrella. Si l'ID est partagé pour une transaction, la valeur correspondante du formateur est « ID_SHARED », sinon « - » est affiché dans le journal des accès.
%[	x-spoofed-ip	Adresse IP source utilisée pour l'usurpation d'adresses IP par le proxy.
%)	x-proxy-instance-id	ID d'instance du proxy si le mode haute performance est activé, sinon un tiret est consigné.
%(	cs-domain-map	Nom de domaine résolu à l'aide de la carte de domaine.
%X#11#	ext_auth_sgt	Paramètre de champ personnalisé pour les étiquettes Groupe sécurisé utilisées dans les intégrations ISE.
%$	informations de déchiffrement	Informations de chiffrement des deux étapes de la transaction. (Client-proxy cipher info##proxy-server cipher info). Les informations dans la séquence ci-dessous - <ciphername>, <protocol version>, Kx=<key exchange>, Au=<authentication>, Enc=<symmetric encryption method>, Mac=<message authentication code>

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%:<1	x-p2s-first-byte-time	Le temps entre le moment où le proxy Web commence à se connecter au serveur et le moment où il est en mesure d'écrire pour la première fois sur le serveur. Si le proxy Web doit se connecter à plusieurs serveurs pour terminer la transaction, il fait la somme de ces temps.
%:<a	x-p2p-auth-wait-time	Temps d'attente pour recevoir la réponse du processus d'authentification du proxy Web, après l'envoi de la demande par le proxy Web.
%:<b	x-p2s-body-time	Temps d'attente pour écrire le corps de la demande sur le serveur après l'en-tête.
%:<d	x-p2p-dns-wait-time	Temps nécessaire au proxy Web pour envoyer la demande DNS au processus DNS du proxy Web.
%:<h	x-p2s-header-time	Temps d'attente pour écrire l'en-tête de demande au serveur après le premier octet
%:<r	x-p2p-reputation- wait-time	Temps d'attente pour recevoir la réponse des filtres de réputation Web, après l'envoi de la demande par le proxy Web.
%:<s	x-p2p-asw-req- wait-time	Temps d'attente pour recevoir le verdict du processus de protection contre les logiciels espions du proxy Web, après l'envoi de la demande par le proxy.
%:>1	x-s2p-first-byte-time	Temps d'attente du premier octet de réponse du serveur
%:>a	x-p2p-auth-svc-time	Temps d'attente pour recevoir la réponse du processus d'authentification du proxy Web, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:>b	x-s2p-body-time	Temps d'attente du corps de la réponse complet après la réception de l'en-tête
%:>c	x-p2p-fetch-time	Temps requis par le proxy Web pour lire une réponse à partir du cache du disque.
%:>d	x-p2p-dns-svc-time	Temps que le processus DNS du proxy Web met à renvoyer un résultat DNS au proxy Web.
%:>h	x-s2p-header-time	Temps d'attente de l'en-tête du serveur après le premier octet de réponse
%:>g		Informations sur la latence d'établissement de la liaison du serveur SSL
%o	-	Quota de temps consommé.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
% O	-	Quota de volume consommé.
%X#41#	x-bw-info	Niveau de contrôle de quota de bande passante appliqué, numéro de canal de bande passante mappé sur une requête, limite de quota de bande passante configurée et profil de quota de bande passante utilisé (level-pipe_no-quota_limit-quota_profile).
%:>r	x-p2p-reputation-svc- time	Le temps d'attente pour recevoir le verdict des filtres de réputation Web, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:>s	x-p2p-asw-req-svc- time	Temps d'attente pour recevoir le verdict du processus de protection contre les logiciels espions du proxy Web, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:1<	x-c2p-first-byte-time	Temps d'attente du premier octet de demande de la nouvelle connexion client
%:1>	x-p2c-first-byte-time	Temps d'attente pour le premier octet écrit sur le client.
%:A<	x-p2p-avc-svc-time	Temps d'attente pour recevoir la réponse du processus l'AVC, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:A>	x-p2p-avc-wait-time	Temps d'attente pour recevoir la réponse du processus AVC, après l'envoi de la demande par le proxy Web.
%:b<	x-c2p-body-time	Temps d'attente pour le corps complet du client.
%:b>	x-p2c-body-time	Temps d'attente pour le corps complet du document écrit au client
%:C<	x-p2p-dca-resp- svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse de contenu dynamique, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:C>	x-p2p-dca-resp- wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse de contenu dynamique, après l'envoi de la demande par le proxy Web.
%:h<	x-c2p-header-time	Temps d'attente pour l'en-tête client complet après le premier octet
%:h>	x-p2c-header-time	Temps d'attente pour l'en-tête complet écrit sur le client

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%:m<	x-p2p-mcafee-resp- svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse McAfee, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:m>	x-p2p-mcafee-resp- wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse McAfee, après l'envoi de la demande par le proxy Web.
%:p<	x-p2p-sophos-resp- svc-time	Temps d'attente avant de recevoir le verdict du moteur d'analyse Sophos, notamment le temps nécessaire au proxy Web pour envoyer la demande.
%:p>	x-p2p-sophos-resp- wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse Sophos, après l'envoi de la demande par le proxy Web
%:w<	x-p2p-webroot-resp -svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse depuis Webroot, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:w>	x-p2p-webroot-resp-wait- time	Temps d'attente pour recevoir la réponse du moteur d'analyse Webroot, après l'envoi de la demande par le proxy Web.
%aBLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%	x-suspect-user-agent	Agent utilisateur suspect, le cas échéant. Si le proxy Web détermine que l'agent utilisateur est suspect, il le consignera dans ce champ. Sinon, il consigne un trait d'union. Ce champ est écrit entre guillemets dans les journaux d'accès.
%<Referer:	cs(Referer)	Référent
%>Server:	sc(Server)	En-tête du serveur dans la réponse.
%a	c-ip	Adresse IP du client.
%A	cs-username	Nom d'utilisateur authentifié. Ce champ est écrit entre guillemets dans les journaux d'accès.
%b	sc-body-size	Octets envoyés au client par le proxy Web pour le corps du message.
%B	octets	Total des octets utilisés (taille de la requête + taille de la réponse, soit %q + %s).
%c	cs-mime-type	Type de corps de réponse MIME. Ce champ est écrit entre guillemets dans les journaux d'accès.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%C	cs(Cookie)	En-tête de témoin. Ce champ est écrit entre guillemets dans les journaux d'accès.
%d	s-hostname	Adresse IP de la source de données ou du serveur.
%]	Header_profile	Nom du profil de réécriture de l'en-tête HTTP.
%D	x-acltag	Balise de décision ACL.
%e	x-elapsed-time	Temps écoulé en millisecondes. Pour le trafic TCP, il s'agit du temps écoulé entre l'ouverture et la fermeture de la connexion HTTP. Pour le trafic UDP, il s'agit du temps écoulé entre l'envoi du premier datagramme et le moment où le dernier datagramme peut être accepté. Une valeur de temps écoulé élevée pour le trafic UDP peut indiquer qu'une valeur de délai d'expiration élevée et une association UDP de longue durée ont permis d'accepter des datagrammes plus longtemps que nécessaire.
%E	x-error-code	Numéro de code d'erreur qui peut aider l'assistance client à résoudre la raison de l'échec d'une transaction.(
%f	cs(X-Forwarded-For)	En-tête X-Forwarded-For.
%F	c-port	Port source du client
%g	cs-auth-group	Noms de groupes autorisés. Ce champ est écrit entre guillemets dans les journaux d'accès. Ce champ est utilisé pour résoudre les problèmes de politique ou d'authentification afin de déterminer si un utilisateur correspond au bon groupe ou à la bonne politique.
%G		Horodatage lisible par l'homme.
%h	sc-http-status	Code de réponse HTTP.
%H	s-hierarchy	Récupération de la hiérarchie.
%i	x-icap-server	Adresse IP du dernier serveur ICAP contacté lors du traitement de la demande.
%I	x-transaction-id	ID de transaction.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%j	DCF	

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
		Ne pas mettre en cache le code de réponse; indicateurs DCF. Descriptions des codes de réponse : • Code de réponse en fonction de la demande du client : • 1 = la demande comportait un en-tête « no-cache ». • 2 = La mise en cache n'est pas autorisée pour la demande. • 4 = Il manque l'en-tête « Variant » dans la requête. • 8 = Nom d'utilisateur ou phrase secrète requis pour la demande de l'utilisateur. • 20 = Réponse pour la méthode HTTP indiquée. • Code de réponse basé sur la réponse reçue par l'appliance : • id="li_7443F05D141F4D9FB788FD416697DB65"> 40 = La réponse contient l'en-tête « Cache-Control: private ». • 80 = La réponse contient l'en-tête « Cache-Control: no-store ». • 100 = La réponse indique que la demande était une interrogation. • 200 = La réponse a une faible valeur « Expires ». • 400 = La réponse n'a pas d'en-tête « Last Modified ». • 1000 = La réponse expire immédiatement. • 2000 = Le fichier de réponse est trop volumineux pour être mis en cache. • 20000 = Une nouvelle copie du fichier existe. • 40000 = La réponse comporte des valeurs incorrectes ou non valides dans l'en-tête « Vary ». • 80000 = La réponse nécessite l'utilisation de témoins.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
		• 100000 = Code d'ÉTAT HTTP non mis en cache • 200000 = L'objet reçu par l'appliance est incomplet (en fonction de la taille). • 800000 = Les bandes de fin de réponse indiquent qu'il n'y a pas de mise en cache. • 1000000 = La réponse doit être réécrite.
%k	s-ip	Adresse IP de la source de données (adresse IP du serveur) Cette valeur est utilisée pour déterminer un demandeur lorsque l'adresse IP est signalée par un périphérique de détection d'intrusion sur votre réseau. Vous permet de localiser un client qui a visité une adresse IP qui a été ainsi marquée.
%l	user-type	Type d'utilisateur, local ou distant.
%L	x-local_time	Demandez l'heure locale dans un format lisible par l'homme : JJ/MMM/AAAA : hh:mm:ss +nnnn. Ce champ est écrit entre guillemets dans les journaux d'accès. L'activation de ce champ vous permet de corréler les journaux aux problèmes sans avoir à calculer l'heure locale à partir de l'heure ancienne pour chaque entrée de journal.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%m	cs-auth-mechanism	Utilisé pour résoudre les problèmes d'authentification. Mécanisme d'authentification utilisé pour la transaction Les valeurs possibles sont les suivantes : • **BASIC.** Le nom d'utilisateur a été authentifié à l'aide du schéma d'authentification de base. • **NTLMSSP.** Le nom d'utilisateur a été authentifié à l'aide du schéma d'authentification NTLMSSP. • **NEGOTIATE.** Le nom d'utilisateur a été authentifié à l'aide du schéma d'authentification Kerberos. • **SSO_TUI.** Le nom d'utilisateur a été obtenu en faisant correspondre l'adresse IP du client à un nom d'utilisateur authentifié à l'aide d'une identification d'utilisateur transparente. • **SSO_ISE.** L'utilisateur a été authentifié par un serveur ISE. (Le journal indique GUEST (INVITÉ) s'il est choisi comme mécanisme de secours pour l'authentification ISE.) • **SSO_ASA.** L'utilisateur est un utilisateur distant et le nom d'utilisateur a été obtenu auprès d'un Cisco ASA à l'aide de Secure Mobility. • **FORM_AUTH.** L'utilisateur saisit les justificatifs d'authentification dans un formulaire dans le navigateur Web lorsqu'il accède à une application. • **GUEST.** L'utilisateur a échoué à l'authentification et a obtenu l'accès en tant qu'invité.
%M	CMF	Indicateurs d'échec du cache : indicateurs CMF.
%N	s-computerName	Nom du serveur ou nom de l'hôte de destination. Ce champ est écrit entre guillemets dans les journaux d'accès.
%p	s-port	Numéro du port de destination.
%P	cs-version	Protocole.
%q	cs-bytes	Taille de la demande (en-têtes + corps)
%r	x-req-first-line	Première ligne de la demande : méthode de demande, URI.
%s	sc-bytes	Taille de la réponse (en-tête + corps)

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%t	Horodatage	Horodatage sous UNIX. **Remarque :** si vous souhaitez utiliser un analyseur de journaux tiers pour lire et analyser les journaux d'accès W3C, vous devrez peut-être inclure le champ « timestamp ». La plupart des analyseurs de journaux ne comprennent l'heure que dans le format fourni par ce champ.
%u	cs(User-Agent)	Agent utilisateur. Ce champ est écrit entre guillemets dans les journaux d'accès. Ce champ permet de déterminer si une application échoue à l'authentification et/ou nécessite des autorisations d'accès différentes.
%U	cs-uri	URI de la demande.
%v	date	Date au format AAAA-MM-JJ.
%V	de temps	Heure au format HH:MM:SS.
%w	sc-result-code	Code de résultat. Par exemple : TCP_MISS, TCP_HIT.
%W	sc-result-code-denial	Code de résultat refusé.
%x	x-latency	Latence.
%X0	x-resp-dvs-scanverdict	Verdict unifié de l'analyse de protection contre les programmes malveillants côté réponse qui fournit le *numéro de catégorie de programmes malveillants*, quel que soit le moteur d'analyse activé. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur. Ce champ est écrit entre guillemets dans les journaux d'accès.
%X1	x-resp-dvs-threat-name	Verdict unifié de l'analyse de protection contre les programmes malveillants côté réponse qui fournit le *nom du programme malveillant*, quel que soit le moteur d'analyse activé. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur. Ce champ est écrit entre guillemets dans les journaux d'accès.
%X2	x-req-dvs-scanverdict	Verdict de l'analyse DVS côté demande
%X3	x-req-dvs-verdictname	Nom du verdict DVS côté demande

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%X4	x-req-dvs-threat-name	Nom de la menace DVS côté demande
%X6	x-as-malware-threat-name	Indique si l'analyse adaptative a bloqué la transaction sans faire appel au moteur d'analyse de protection contre les programmes malveillants. Les valeurs possibles sont les suivantes : • **1.** La transaction a été bloquée. • **0.** La transaction n'a pas été bloquée. Cette variable est incluse dans les informations sur le verdict de l'analyse (entre les crochets à la fin de chaque entrée du journal des accès).
%XA	x-webcat-resp-code- abbr	Verdict de catégorie d'URL déterminé lors de l'analyse côté réponse, en abrégé. S'applique uniquement au moteur de filtrage d'URL Cisco Web Usage Controls.
%Xb	x-avc-behavior	Comportement de l'application Web identifié par le moteur AVC.
%XB	x-avg-bw	Bande passante moyenne de l'utilisateur si les limites de bande passante sont définies par le moteur AVC.
%XC	x-webcat-code-abbr	Abréviation de catégorie d'URL de la catégorie d'URL personnalisée attribuée à la transaction.
%Xd	x-mcafee-scanverdict	Identifiant spécifique à McAfee : (verdict d'analyse)
%Xe	x-mcafee-filename	Identifiant spécifique à McAfee : (Nom du fichier produisant le verdict) ce champ est écrit avec des guillemets dans les journaux d'accès.
%Xf	x-mcafee-av-scanerror	Identifiant propre à McAfee : (erreur d'analyse).
%XF	x-webcat-code-full	Nom complet de la catégorie d'URL attribuée à la transaction. Ce champ est écrit entre guillemets dans les journaux d'accès.
%Xg	x-mcafee-av-detecttype	Identifiant spécifique à McAfee : (type de détection).
%XG	x-avc-reqhead-scanverdict	Verdict de l'en-tête de la demande AVC
%Xh	x-mcafee-av-virustype	Identifiant spécifique à McAfee : (type de virus)
%XH	x-avc-reqbody- scanverdict	Verdict du corps de la demande AVC.
%Xi	x-webroot-trace-id	Identifiant d'analyse spécifique à Webroot : (ID Trace)

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%Xj	x-mcafee-virus-name	Identifiant spécifique à McAfee : (nom du virus) Ce champ est écrit entre guillemets dans les journaux d'accès.
%Xk	x-wbrs-threat-type	Type de menace pour la réputation Web.
%XK	x-wbrs-threat-reason	Motif de la menace pour la réputation Web.
%Xl	x-ids-verdict	Verdict d'analyse de la politique de sécurité des données de Cisco. Si ce champ est inclus, il affichera le verdict IDS, ou « 0 » si l'IDS était actif mais le document analysé à jour, ou « - » si aucune politique IDS n'était active pour la demande.
%XL	x-webcat-resp-code- full	Verdict de catégorie d'URL déterminé lors de l'analyse côté réponse, nom complet. S'applique uniquement au moteur de filtrage d'URL Cisco Web Usage Controls.
%XM	x-avc-resphead- scanverdict	Verdict de l'en-tête de réponse AVC
%Xn	x-webroot-threat-name	Identifiant spécifique à Webroot : (Nom de la menace) Ce champ est écrit entre guillemets dans les journaux d'accès.
%XN	x-avc-reqbody-scanverdict	Verdict du corps de la réponse AVC.
%XO	x-avc-app	Application Web identifiée par le moteur AVC.
%Xp	x-icap-verdict	Verdict de l'analyse du serveur DLP externe
%XP	x-acl-added-headers	En-tête non reconnu. Utilisez ce champ pour consigner des en-têtes supplémentaires dans les demandes des clients. Cela prend en charge le dépannage de systèmes spécialisés qui ajoutent des en-têtes aux demandes des clients pour les authentifier et les rediriger, par exemple YouTube for Schools.
%XQ	x-webcat-req-code- abbr	Verdict de catégorie d'URL prédéfinie déterminé lors de l'analyse côté demande, en abrégé.
%Xr	x-result-code	Informations sur le verdict de l'analyse.
%XR	x-webcat-req-code-full	Verdict de catégorie d'URL déterminé lors de l'analyse côté demande, nom complet.
%Xs	x-webroot-spyid	Identifiant spécifique à Webroot : (ID espion).

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%XS	x-request-rewrite	Verdict de l'analyse pour une navigation sécurisée Indique si la recherche sécurisée ou la fonction d'évaluation du contenu du site a été appliquée à la transaction.
%Xt	x-webroot-trr	Identifiant propre à Webroot : [Rapport menaces/risques (TRR)].
%XT	x-bw-throttled	Indicateur qui indique si des limites de bande passante ont été appliquées à la transaction.
%Xu	x-avc-type	Type d'application Web identifié par le moteur AVC.
%Xv	x-webroot-scanverdict	Verdict de l'analyse des programmes malveillants depuis Webroot.
%XV	x-request-source-ip	L'adresse IP en aval lorsque la case « Enable Identification of Client IP Addresses using X-Forwarded-For » (Activer l'identification des adresses IP clientes à l'aide de X-Forwarded-For) est cochée pour les paramètres du proxy Web.
%XW	x-wbrs-score	Score WBRS décodé <-10.0-10.0>.
%Xx	x-sophos-scanerror	Identifiant spécifique à Sophos : (code de retour de l'analyse).
%Xy	x-sophos-file-name	Nom du fichier dans lequel Sophos a trouvé le contenu répréhensible. S'applique uniquement aux réponses détectées par Sophos.
%XY	x-sophos-scanverdict	Identifiant spécifique à Sophos : (verdict de l'analyse).
%Xz	x-sophos-virus-name	Identifiant spécifique à Sophos : (nom de la menace).
%XZ	x-resp-dvs-verdictname	Verdict unifié de l'analyse de protection contre les programmes malveillants côté réponse qui fournit la *catégorie de programmes malveillants* indépendamment des moteurs d'analyse activés. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur. Ce champ est écrit entre guillemets dans les journaux d'accès.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%X#1#	x-amp-verdict	Verdict de l'analyse des fichiers Cisco Secure Endpoint : • 0 : Le fichier n'est pas malveillant. • 1 : Le fichier n'a pas été analysé en raison de son type de fichier. • 2 : L'analyse des fichiers a expiré. • 3 : Erreur de l'analyse. • Supérieur à 3 : Le fichier est malveillant.
%X#2#	x-amp-malware-name	Nom de la menace, comme déterminé par l'analyse des fichiers Cisco Secure Endpoint. « - » indique l'absence de menace.
%X#3#	x-amp-score	Score de réputation résultant de l'analyse des fichiers Cisco Secure Endpoint. Ce score est utilisé uniquement si le service de réputation en nuage n'est pas en mesure de déterminer un verdict clair pour le fichier. Pour en savoir plus, consultez les informations sur le score de menace et le seuil de réputation dans Filtrage de réputation de fichiers et analyse de fichiers, on page 323
%X#4#	x-amp-upload	Indicateur de chargement et de demande d'analyse : « 0 » indique que Cisco Secure Endpoint n'a pas demandé le chargement du fichier pour analyse. « 1 » indique que Cisco Secure Endpoint a demandé le chargement du fichier pour analyse.
%X#5#	x-amp-filename	Nom du fichier en cours de téléchargement et d'analyse.
%X#6#	x-amp-sha	Identifiant SHA-256 de ce fichier.
%y	cs-method	Méthode.
%Y	cs-url	URL complète.
%:e<	x-p2p-amp-svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse Cisco Secure Endpoint , y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:e>	x-p2p-amp-wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse Cisco Secure Endpoint , après l'envoi de la demande par le proxy Web.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
S. O.	x-hierarchy-origin	Code qui décrit le serveur contacté pour récupérer le contenu de la demande (par exemple, DIRECT/www.exemple.com).
S. O.	x-resultcode-httpstatus	Code de résultat et le code de réponse HTTP, séparés par une barre oblique (/).
S. O.	x-archivescan-verdict	Affiche le verdict de l'inspection des archives.
S. O.	x-archivescan-verdict- reason	Détails du fichier bloqué par l'analyse des archives
%XU	S. O.	Pour utilisation future.

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500.
- Interprétation des journaux d'accès W3C, on page 521.

Valeurs de verdict de la recherche de programmes malveillants

Un verdict d'analyse contre les programmes malveillants est une valeur affectée à une requête d'URL ou à une réponse d'un serveur qui détermine la probabilité qu'elle convienne à des programmes malveillants. Les moteurs d'analyse Webroot, McAfee et Sophos renvoient un verdict de recherche de programmes malveillants au moteur DVS pour que ce dernier puisse déterminer s'il faut surveiller ou bloquer l'objet analysé. Chaque verdict d'analyse contre les programmes malveillants correspond à une catégorie de programmes malveillants répertoriée sur la page Access Policies > Reputation and Anti-Malware Settings (Politiques d'accès > Paramètres de protection contre les programmes malveillants et de réputation) lorsque vous modifiez les paramètres de protection contre les programmes malveillants pour une politique d'accès particulière.

La liste suivante présente les différentes valeurs de verdict d'analyse contre les programmes malveillants et chaque catégorie de programmes malveillants correspondante :

Valeur du verdict de l'analyse des programmes malveillants	Catégorie de programmes malveillants
-	Non défini
0	Inconnu
1	Non analysé
2	Délai d'expiration
3	Erreur
4	Impossible à analyser
10	Logiciel espion générique

Valeur du verdict de l'analyse des programmes malveillants	Catégorie de programmes malveillants
12	Objet de l'assistant du navigateur
13	Logiciels publicitaires
14	Moniteur système
18	Supervision de système commercial
19	Composeur automatique
20	Détournement d'identité
21	URL d'hameçonnage
22	Outil de téléchargement de chevaux de Troie
23	Cheval de Troie
24	Cheval de Troie pour hameçonnage
25	Vers
26	Fichier chiffré
27	Virus
33	Autres programmes malveillants
34	API (applications potentiellement indésirables)
35	Abandonné
36	Heuristique des épidémies
37	Fichiers malveillants ou à risque élevé connus

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 500.
- Interprétation des journaux d'accès W3C, on page 521.

Résolution des problèmes de journalisation

CHAPITRE 23

Intégration avec Cisco SecureX et Cisco Threat Response

Cette rubrique contient les sections suivantes :

Intégration de votre appliance à Cisco SecureX ou Cisco Threat Response

Cisco SecureX est une plateforme de sécurité intégrée à tous les produits de sécurité Cisco. Cette solution est native dans le nuage, sans nouvelle technologie à déployer. Cisco SecureX simplifie les exigences de la protection contre les menaces en fournissant une plateforme qui unifie la visibilité, permet l'automatisation et améliore la sécurité sur le réseau, les terminaux, le nuage et les applications. En connectant la technologie dans une plateforme intégrée, Cisco SecureX fournit des informations mesurables, des résultats souhaitables et une collaboration entre les équipes inégalée. Cisco SecureX vous permet d'étendre vos capacités en connectant votre infrastructure de sécurité.

Le service d'intégration de l'appliance à Cisco SecureX ou Cisco Threat Response contient les sections suivantes :

Vous pouvez intégrer votre appliance à Cisco SecureX ou Cisco Threat Response et effectuer les actions suivantes dans Cisco SecureX ou Cisco Threat Response :

- Affichez et envoyez les données Web de plusieurs appliances de votre organisation.
- Identifiez, étudiez et corrigez les menaces observées dans les rapports Web et le suivi.
- Bloquez les URL ou le trafic Web compromis.

- Résoudre rapidement les menaces identifiées et fournir des recommandations de mesures à prendre contre les menaces identifiées.
- Documentez les menaces pour enregistrer l'enquête et permettre l'échange d'informations entre d'autres appliances.
- Bloquez les domaines malveillants, suivez les observations suspectes, lancez un flux de travail d'approbation ou créez un dossier informatique pour mettre à jour la politique Web.

Vous pouvez accéder à Cisco SecureX ou à Cisco Threat Response en utilisant l'URL suivante :

https://securex.us.security.cisco.com/login

Cisco Secure Web Appliance fournit des fonctionnalités avancées de protection contre les menaces qui détectent, bloquent et éliminent les attaques plus rapidement, qui empêchent la perte de données et qui sécurisent les informations importantes en transit avec un chiffrement de bout en bout. Pour en savoir plus sur les observables qui peuvent être enrichies par le module Secure Web Appliance, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX et cliquez sur **En savoir plus**.

Lorsque vous intégrez Cisco Secure Web Appliance à SecureX, les données de suivi Web de Secure Web Appliance sont validées. L'expiration du délai de transaction (60 secondes) se produit en raison du retard de traitement sur Secure Web Appliance, ce qui entraîne un échec de l'intégration. Réduisez la limite de temps d'intégration de 30 jours par défaut à 1 ou 2 jours pour une intégration réussie. Cependant, cette réduction aura une incidence sur l'efficacité de la supervision de Cisco Secure Web Appliance.

Comment intégrer votre appliance à Cisco SecureX ou Cisco Threat Response

Tableau 23 : Comment intégrer votre appliance à Cisco SecureX ou Cisco Threat Response

	Faire ceci	Plus d'informations
Étape 1	Passez en revue les conditions préalables.	Prérequis, à la page 547
Étape 2	Sur votre Secure Web Appliance, activez l'intégration Cisco SecureX ou Cisco Threat Response.	Activez l'intégration de Cisco SecureX ou Cisco Threat Response sur votre Secure Web Appliance Cisco, à la page 547
Étape 3	Sur Cisco SecureX, ajoutez votre appliance en tant que périphérique, enregistrez-la et générez un jeton d'enregistrement.	Pour en savoir plus, consultez https://securex.us.security.cisco.com/help/settings-devices
Étape 4	Sur votre Secure Web Appliance, terminez l'enregistrement de Cisco SecureX ou Cisco Threat Response.	Enregistrement de Cisco SecureX ou de Cisco Threat Response sur Cisco Secure Web Appliance, à la page 548
Étape 5	Confirmer si l'enregistrement a réussi.	Confirmer la réussite de l'enregistrement, à la page 549

	Faire ceci	Plus d'informations
Étape 6	Sur Cisco SecureX, ajoutez le module d'appliance Cisco pour la sécurité du Web.	Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module Secure Web Appliance requis pour l'intégration dans Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Prérequis

Remarque Si vous avez déjà un compte d'utilisateur Cisco Threat Response, vous n'avez pas besoin de créer un compte d'utilisateur Cisco SecureX. Vous pouvez vous connecter à Cisco SecureX à l'aide des informations d'authentification de votre compte d'utilisateur Cisco Threat Response.

- Assurez-vous de créer un compte d'utilisateur dans Cisco SecureX avec des droits d'accès administrateur. Pour créer un nouveau compte d'utilisateur, accédez à la page **Cisco SecureX login** (Connexion à Cisco SecureX) en utilisant l'URL https://securex.us.security.cisco.com/login et cliquez sur **Create a SecureX Sign-on Account** (Créer un compte de connexion SecureX) dans la page de connexion. Si vous ne parvenez pas à créer un nouveau compte d'utilisateur, communiquez avec le service d'assistance technique de Cisco pour obtenir de l'aide.
- [Uniquement si vous n'utilisez pas de serveur proxy.] Assurez-vous d'ouvrir le port HTTPS (entrée et sortie) 443 sur le pare-feu pour les noms de domaine complets suivants afin d'enregistrer votre appliance auprès de Cisco SecureX ou Cisco Threat Response :
  - api-sse.cisco.com (applicable pour les utilisateurs NAM uniquement)
  - api.eu.sse.itd.cisco.com (uniquement applicable aux utilisateurs dans l'Union européenne)
  - api.apj.sse.itd.cisco.com (uniquement applicable aux utilisateurs dans la région APJC)
  - est.sco.cisco.com (applicable aux utilisateurs APJC, UE et NAM)

Activez l'intégration de Cisco SecureX ou Cisco Threat Response sur votre Secure Web Appliance Cisco

Étape 1 Connectez-vous à votre appliance.

Étape 2 Sélectionnez **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 3 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 4 Cochez la case **Enable** (Activer).

Étape 5 Choisissez le serveur Cisco SecureX ou Cisco Threat Response requis pour connecter votre appliance à Cisco SecureX ou Cisco Threat Response.

Étape 6 Envoyez et validez vos modifications.

Étape 7 Attendez quelques minutes et vérifiez si le bouton **Register** (Enregistrer) apparaît sur votre appliance.

Prochaine étape

Enregistrez votre appliance sur Cisco SecureX ou Cisco Threat Response. Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Enregistrement de Cisco SecureX ou de Cisco Threat Response sur Cisco Secure Web Appliance

Étape 1 Accédez à **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 2 Dans les **Cloud Services Settings** (Paramètres des services en nuage), saisissez le jeton d'enregistrement, puis cliquez sur **Register** (Enregistrer).

Remarque Pour enregistrer Cisco SecureX ou Cisco Threat Response à l'aide de l'interface de ligne de commande, utilisez la commande `cloudserviceconfig`.

Prochaine étape

Confirmer la réussite de l'enregistrement, à la page 549

Enregistrement de Cisco Secure Web Appliance sur le portail Security Service Exchange (SSE) à l'aide de la licence Smart

Lorsque vous effectuez une mise à niveau vers AsyncOS 14.x, les services Cisco Cloud sont automatiquement activés si l'appliance est déjà enregistrée dans Cisco Smart Software Manager. Suivez les étapes ci-dessous pour ajouter votre appliance au portail SSE.

Étape 1 Planifiez une fenêtre de maintenance.

Étape 2 Accédez à **System Administration** > **Smart Software Licensing** (Administration système > Licences logicielles Smart).

Étape 3 Dans la liste déroulante **Action**, sélectionnez **Deregister** (Annuler l'enregistrement) et cliquez sur **Go** (OK).

Étape 4 Supprimez toutes les entrées SWA du portail SSE.

Étape 5 Accédez à **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 6 Cochez la case **Enable Cisco Cloud Services** (Activer les services Cisco Cloud).

Étape 7 Cliquez sur **Enable** (Activer).

Étape 8 Envoyez et validez vos modifications.

Étape 9 Collez le jeton d'enregistrement.

Étape 10 Cliquez sur **Register** (Enregistrer).

Confirmer la réussite de l'enregistrement

- Sur la plateforme Security Services Exchange, confirmez la réussite de l'enregistrement en vérifiant l'état dans la plateforme Security Services Exchange.
- Sur Cisco SecureX, accédez à la page **Devices** (Périphériques) et affichez le Secure Web Appliance qui a été enregistré auprès de la plateforme Security Services Exchange.

Remarque Si vous souhaitez passer à un autre serveur Cisco SecureX ou Cisco Threat Response (par exemple, « Europe - api.eu.sse.itd.cisco.com »), vous devez d'abord annuler l'enregistrement de votre appliance auprès de Cisco SecureX ou de Cisco Threat Response, puis suivre les étapes mentionnées dans Comment intégrer votre appliance à Cisco SecureX ou Cisco Threat Response, à la page 546.

Après avoir intégré votre appliance à Cisco SecureX ou Cisco Threat Response, vous n'avez pas besoin d'intégrer votre appliance Cisco de gestion de la sécurité à Cisco SecureX ou Cisco Threat Response.

Après l'enregistrement réussi de votre appliance sur la plateforme Security Services Exchange, ajoutez le module Web Secure Web Appliance sur Cisco SecureX. Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Activation du portail de services infonuagiques Cisco Secure Web Appliance

Étape 1 Connectez-vous à votre Secure Web Appliance.

Étape 2 Sélectionnez **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 3 Cliquez sur **Enable** (Activer).

Étape 4 Cochez la case **Enable Cisco Cloud Services** (Activer les services Cisco Cloud).

Étape 5 Choisissez le serveur Cisco Secure requis pour connecter votre Secure Web Appliance au portail de services Cisco Cloud.

Étape 6 Envoyez et validez vos modifications.

Étape 7 Attendez quelques minutes et vérifiez si le bouton **Register** (Enregistrer) apparaît sur la page **Cloud Services Settings** (Paramètres des services Cisco Cloud).

Remarque Pour activer le portail de services Cisco Cloud à l'aide de l'interface de ligne de commande, utilisez la commande `cloudserviceconfig`.

Prochaine étape

Enregistrer votre Secure Web Appliance sur le portail des services Cisco Cloud. Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Enregistrement de Secure Web Appliance sur le portail des services Cisco Cloud

Étape 1 Accédez à **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 2 Saisissez le jeton d'enregistrement dans les paramètres des services Cisco Cloud et cliquez sur **Register** (Enregistrer) .

Remarque Pour enregistrer votre Secure Web Appliance auprès du portail des services Cisco Cloud à l'aide de l'interface de ligne de commande, utilisez la commande `cloudserviceconfig`.

Vous ne pouvez pas désactiver ou annuler l'enregistrement des services Cisco Cloud si une licence Smart est enregistrée sur votre appliance.

Analyse des menaces à l'aide du ruban Cisco SecureX

Remarque Lorsque vous passez à AsyncOS 14.0 ou à des versions antérieures, **Casebook** fait partie du ruban Cisco SecureX.

Cisco SecureX prend en charge un ensemble distribué de fonctionnalités qui unifient la visibilité, permettent l'automatisation, accélèrent les flux de travail de réponse aux incidents et améliorent la recherche de menaces. Ces fonctionnalités distribuées sont présentées sous forme d'applications (applis) et d'outils dans le ruban Cisco SecureX.

Cette rubrique contient les sections suivantes :

- Accès au ruban Cisco SecureX, à la page 551
- Ajout d'observable à Casebook pour l'analyse des menaces à l'aide du menu du ruban et du tableau croisé dynamique de Cisco SecureX, à la page 552

Vous trouverez le ruban Cisco SecureX dans le volet inférieur de la page et il persiste lorsque vous vous déplacez entre le tableau de bord et les autres produits de sécurité de votre environnement. Le ruban Cisco SecureX se compose des icônes et des éléments suivants :

- Développer/Réduire le ruban
- Accueil

- Application Casebook
- Application Incidents
- Application Orbital
- Case de recherche d'enrichissement
- Recherche d'observables
- Paramètres

Pour en savoir plus sur le ruban Cisco SecureX, consultez la page https://securex.us.security.cisco.com/help/ribbon.

Accès au ruban Cisco SecureX

Avant de commencer

Assurez-vous de remplir tous les préalables mentionnés dans Prérequis, à la page 547.

Remarque Supposons que vous ayez déjà configuré les versions antérieures de **Casebook** pour AsyncOS. Vous devez créer un nouvel **ID client** et un nouveau **secret client** dans le client API Cisco SecureX avec des étendues supplémentaires, comme mentionné dans la procédure suivante.

Vous pouvez faire glisser le Cisco SecureX Ribbon, placé dans le volet inférieur de la page, depuis la droite en utilisant le bouton  .

Étape 1 Connectez-vous à la nouvelle interface Web de votre appliance. Pour en savoir plus, consultez Interprétation des pages de rapports Web sur la nouvelle interface Web, à la page 429.

Étape 2 Cliquez sur le ruban Cisco SecureX.

Étape 3 Créez un **ID client** et un **secret client** dans les **clients API SecureX**. Pour en savoir plus sur la génération d'informations d'authentification de client API, consultez Création d'un client API.

Lors de la création d'un ID client et d'un mot de passe client, veillez à choisir les étendues suivantes :

- recueil
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profil
- private-intel

- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital (si vous y avez accès)

Étape 4 Saisissez le nom d'utilisateur et le mot de passe client obtenus à l'étape 3 dans la boîte de dialogue **Login to use SecureX Ribbon** (Se connecter pour utiliser le ruban SecureX) dans votre appliance.

Étape 5 Sélectionnez le serveur Cisco SecureX requis dans la boîte de dialogue **Login to use SecureX Ribbon** (Se connecter pour utiliser le ruban SecureX).

Étape 6 Cliquez sur **Authenticate** (Authentifier).

Remarque Si vous souhaitez modifier l'ID du client, le mot de passe du client et le serveur Cisco SecureX, faites un clic droit sur le ruban Cisco SecureX et ajoutez les détails.

Prochaine étape

Ajout d'observable à Casebook pour l'analyse des menaces à l'aide du menu du ruban et du tableau croisé dynamique de Cisco SecureX, à la page 552

Ajout d'observable à Casebook pour l'analyse des menaces à l'aide du menu du ruban et du tableau croisé dynamique de Cisco SecureX

Avant de commencer

Assurez-vous d'obtenir l'ID client et le mot de passe client pour accéder aux widgets du ruban et du menu croisé dynamique de Cisco SecureX sur votre appliance. Pour en savoir plus, consultez Accès au ruban Cisco SecureX, à la page 551.

Étape 1 Connectez-vous à la nouvelle interface Web de votre appliance. Pour en savoir plus, consultez Interprétation des pages de rapports Web sur la nouvelle interface Web, à la page 429.

Étape 2 Accédez à la page **Web Reporting** (Rapports Web), cliquez sur le bouton de menu croisé dynamique  à côté de l'observable requis (par exemple, bit.ly).

Procédez comme suit:

- Cliquez sur le bouton  pour ajouter un observable au dossier actif.
- Cliquez sur le bouton  pour ajouter l'observable au nouveau dossier.

Remarque

Utilisez le bouton du menu croisé dynamique pour faire basculer un observable par rapport à d'autres périphériques enregistrés sur le portail (par exemple, Cisco Secure Endpoint) afin de mener une recherche pour l'analyse des menaces.

Étape 3 Passez le curseur sur l'icône et cliquez sur le bouton pour ouvrir **Casebook**. Vérifiez si l'observable est ajouté à un nouveau dossier ou à un dossier existant.

Étape 4 (Facultatif) Cliquez sur le bouton pour ajouter un titre, une description ou des remarques à **Casebook**.

Remarque Vous pouvez rechercher des observables pour l'analyse des menaces de deux manières différentes :

- Cliquez sur la zone de recherche **Enrichment** (Enrichissement) dans le ruban Cisco SecureX et recherchez les observables.
- Cliquez sur l'icône **Casebook** dans le ruban Cisco SecureX et recherchez les observables dans le champ de recherche 

.

Pour en savoir plus sur le ruban Cisco SecureX, consultez la page https://securex.us.security.cisco.com/help/ribbon.

CHAPITRE 24

Effectuer les tâches d'administration du système

Cette rubrique contient les sections suivantes :

Survol de l'administration du système

L'appliance série S offre divers outils pour la gestion du système. Les fonctionnalités de l'onglet System Administration (Administration système) vous aident à gérer les tâches suivantes :

- Configuration des appliances
- Clés de fonctionnalité
- Ajout, modification et suppression de comptes d'utilisateur
- Mises à jour et mises à niveau du logiciel AsyncOS
- Heure système

Enregistrement, chargement et réinitialisation de la configuration de l'appliance

Tous les paramètres de configuration dans Secure Web Appliance sont gérés à l'aide d'un fichier de configuration XML unique.

Affichage et impression de la configuration de l'appliance

Étape 1 Choisissez **System Administration > Configuration Summary** (Administration système > Résumé de la configuration).

Étape 2 Affichez ou imprimer la page du sommaire de la configuration, le cas échéant.

Enregistrement du fichier de configuration de l'appliance

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Remplissez les options du fichier de configuration .

Option	Description
Indiquer une option de gestion de fichiers	Choisissez le mode de traitement du fichier de configuration généré : • Téléchargez le fichier sur l'ordinateur local pour l'afficher ou l'enregistrer. • **Enregistrez le fichier sur cette appliance** (wsa_exemple.com). • **Email file to** (Envoyer le fichier par courriel à) : indiquez une ou plusieurs adresses de courriel.
Indiquez une option de gestion de la phrase secrète	• **Masquer les phrases secrètes dans les fichiers de configuration** – Les phrases secrètes d'origine sont remplacées par « ***** » dans le fichier exporté ou enregistré. Veuillez noter que les fichiers de configuration avec des phrases secrètes masquées ne peuvent pas être chargés directement dans AsyncOS pour le Web. • **Chiffrer les phrases secrètes dans les fichiers de configuration** : si le mode FIPS est activé, cette option est disponible. Consultez Activation ou désactivation du mode FIPS , on page 605 pour obtenir des renseignements sur l'activation du mode FIPS.

Option	Description
Sélectionner une option de nom de fichier	Choisissez le nom du fichier de configuration : • **Utiliser le nom de fichier généré par le système** • **Utiliser un nom de fichier défini par l'utilisateur**

Étape 3 Cliquez sur **Submit** (Soumettre).

Chargement du fichier de configuration de l'appliance

Caution Le chargement de la configuration supprimera définitivement tous vos paramètres de configuration actuels. Il est fortement recommandé d'enregistrer votre configuration avant d'effectuer ces actions.

Nous vous déconseillons de charger des configurations d'une version précédente dans la dernière version. Vous pouvez conserver les paramètres de configuration en mettant à niveau les chemins.

Les fichiers de configuration chargés avec des modifications manuelles peuvent entraîner des problèmes de performances et fonctionnels.

Note Si un fichier de configuration compatible est basé sur une version de l'ensemble de catégories d'URL plus ancienne que la version actuellement installée sur l'appliance, les politiques et les identités du fichier de configuration peuvent être modifiées automatiquement.

Note Si vous rencontrez une erreur de validation de certificat lors du chargement du fichier de configuration, chargez l'autorité de certification racine du certificat dans le répertoire racine approuvé de Secure Web Appliance, puis chargez à nouveau le fichier de configuration. Pour savoir comment charger l'autorité de certification racine, consultez Certificate Management, on page 608.

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Choisissez les options Load Configuration (Charger la configuration) et un fichier à charger. Remarque :

Note
- Les fichiers dont la phrase secrète est masquée ne peuvent pas être chargés.
- Les fichiers doivent avoir l'en-tête suivant :

  `<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">`

  et une section de configuration correctement mise en forme :

  `<config>` ... *vos informations de configuration dans un fichier XML valide* `</config>`

Étape 3 Cliquez sur **Load** (Charger).

Étape 4 Lisez l'avertissement qui s'affiche. Si vous comprenez les conséquences de cette procédure, cliquez sur **Continue** (Continuer).

Réinitialisation de la configuration de l'appliance aux valeurs par défaut

Vous pouvez choisir de conserver ou non les paramètres réseau existants lorsque vous réinitialisez la configuration de l'appliance.

Cette action ne nécessite pas de validation.

Before you begin

Enregistrez votre configuration à un emplacement hors de l'appliance.

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Faites défiler la liste vers le bas pour afficher la section **Reset Configuration** (Réinitialiser la configuration).

Étape 3 Lisez les informations sur la page et sélectionnez les options.

Étape 4 Cliquez sur **Reset** (Réinitialiser).

Enregistrement de la sauvegarde du fichier de configuration

La fonction de sauvegarde du fichier de configuration enregistre la configuration de l'appliance à chaque validation et envoie le fichier de configuration précédent avant l'actuel à un serveur de sauvegarde distant par FTP ou SCP.

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Cochez la case **Enable Config Backup** (Activer la sauvegarde de la configuration).

Étape 3 Choisissez **Yes** (Oui) pour inclure la phrase secrète dans le fichier de configuration. Vous pouvez également choisir **No** (Non) pour exclure la phrase secrète du fichier de configuration.

Étape 4 Choisissez la méthode de récupération. Les options disponibles sont les suivantes :

- FTP on Remote Server (FTP sur le serveur distant) : saisissez le nom d'hôte, le répertoire, le nom d'utilisateur et la phrase secrète du FTP.
- SCP on Remote Server (SCP sur le serveur distant) : saisissez le nom d'hôte, le numéro de port, le répertoire et le nom d'utilisateur SCP.
- Host Key Checking (Vérification de la clé de l'hôte) : le SSH gère et vérifie automatiquement une base de données des identifications pour tous les hôtes avec lesquels il a été utilisé. Les clés d'hôte sont stockées dans le répertoire de base de l'utilisateur, à savoir le répertoire */.ssh/known_hosts*.

  Si vous sélectionnez **SCP on Remote Server** (SCP sur le serveur distant), puis sélectionnez **Enable Host Key Checking** (Activer la vérification de la clé hôte), vous disposerez des options suivantes :

  - Automatic (Automatique) : la clé d'hôte sera définie automatiquement par Secure Web Appliance.
  - Manual (Manuel) : l'utilisateur peut saisir la clé d'hôte manuellement.

Une fois les modifications envoyées, l'appliance Cisco pour la sécurité du Web fournit une ou plusieurs clés SSH à ajouter au fichier de clés autorisées sur l'hôte distant, afin que les fichiers de configuration puissent être chargés de l'appliance Cisco pour la sécurité du Web vers l'hôte distant. Par conséquent, SSH gère et vérifie une base de données contenant les informations d'identification de tous les hôtes auxquels il s'est connecté. Les clés d'hôte sont stockées dans le répertoire de base de l'utilisateur, à savoir le répertoire */.ssh/known_hosts*.

Étape 5 Cliquez sur **Submit** (Soumettre).

Vous pouvez également activer la fonction de sauvegarde du fichier de configuration en utilisant la commande de l'interface de ligne de commande `configbackup`

Licenses Cisco Secure Web Appliance

Utilisation des clés de fonctionnalité

Les clés de fonctionnalité activent des fonctionnalités spécifiques sur votre système. Les clés sont spécifiques au numéro de série de votre appliance (vous ne pouvez pas réutiliser une clé d'un système sur un autre système).

Affichage et mise à jour des clés de fonctionnalité

Étape 1 Choisissez **System Administration > Feature Keys** (Administration système > Clés de fonctionnalité).

Étape 2 Pour actualiser la liste des clés en attente, cliquez sur **Check for New Keys** (Rechercher de nouvelles clés) afin d'actualiser la liste des clés en attente.

Étape 3 Pour ajouter une nouvelle clé de fonctionnalité manuellement, collez ou saisissez la clé dans le champ Feature Key (Clé de fonctionnalité) et cliquez sur **Submit Key** (Envoyer la clé). Si la clé de fonctionnalité est valide, elle est ajoutée à l'affichage.

Étape 4 Pour activer une nouvelle clé de fonctionnalité à partir de la liste Pending Activation (Activation en attente), cochez la case « Select » (Sélectionner) et cliquez sur **Activate Selected Keys** (Activer les clés sélectionnées).

Vous pouvez configurer votre appliance de manière à télécharger et installer automatiquement les nouvelles clés dès qu'elles sont émises. Dans ce cas, la liste Pending Activation (Activation en attente) sera toujours vide. Vous pouvez demander à AsyncOS de rechercher de nouvelles clés à tout moment en cliquant sur le bouton **Check for New Keys** (Rechercher les nouvelles clés), même si vous avez désactivé la vérification automatique dans la page Feature Key Settings (Paramètres des clés de fonctionnalité).

Modification des paramètres de mise à jour des clés de fonctionnalité

La page des paramètres des clés de fonctionnalité permet de contrôler si votre appliance vérifie et télécharge de nouvelles clés de fonctionnalité, et si ces clés sont activées automatiquement.

Étape 1 Choisissez **System Administration > Feature Key Settings** (Administration système > Paramètres des clés de fonctionnalité).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Modifiez les paramètres des clés de fonctionnalité au besoin.

Option	Description
Transmission automatique des clés de fonctionnalité	Options permettant de vérifier et de télécharger automatiquement les clés de fonctionnalité et d'activer automatiquement les clés de fonctionnalité téléchargées. Les vérifications automatiques sont normalement effectuées une fois par mois, mais ce nombre passe à une fois par jour si une clé de fonctionnalité doit expirer dans moins de 10 jours et à une fois par jour après l'expiration de la clé, pendant un maximum d'un mois. Après un mois, la clé expirée n'est plus incluse dans la liste des clés sur le point d'expirer et qui ont expiré.

Étape 4 Envoyez et validez vos modifications.

Gestion des licences Smart Software

Survol

Les licences logicielles Smart vous permettent de gérer et de surveiller les licences Cisco Secure Web Appliance. Pour activer les licences logicielles Smart, vous devez enregistrer votre appliance auprès de Cisco Smart Software Manager (CSSM), la base de données centralisée contenant les détails de la licence pour tous

les produits Cisco que vous achetez et utilisez. Grâce aux licences Smart, vous pouvez vous inscrire avec un jeton unique plutôt que de les enregistrer individuellement sur le site Web à l'aide des clés d'autorisation de produit (PAK).

Une fois l'appliance enregistrée, vous pouvez suivre vos licences d'appliance et surveiller l'utilisation des licences sur le portail CSSM. L'agent Smart installé sur l'appliance connecte cette dernière au portail CSSM et transmet les informations d'utilisation des licences au portail CSSM pour le suivi de la consommation.

Consultez https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur Cisco Smart Software Manager.

Remarque AsyncOS version 15.0 est la dernière version à prendre en charge la licence classique. Les prochaines versions ne prendront en charge que les licences Smart.

Avant de commencer

- Assurez-vous que votre appliance est connectée à Internet.
- Communiquez avec l'équipe commerciale de Cisco pour créer un compte Smart dans le portail Cisco Smart Software Manager (https://software.cisco.com/#module/SmartLicensing) ou installez un satellite Cisco Smart Software Manager sur votre réseau.

  Consultez https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur la création de compte d'utilisateur ou l'installation d'un satellite Cisco Smart Software Manager.

  Pour les utilisateurs qui ne souhaitent pas envoyer directement les informations d'utilisation des licences sur Internet, le satellite Smart Software Manager peut être installé sur site et fournit un sous-ensemble de la fonctionnalité CSSM. Une fois que vous avez téléchargé et déployé l'application satellite, vous pouvez gérer les licences localement et en toute sécurité sans envoyer de données au CSSM sur Internet. Le satellite CSSM transmet périodiquement les informations au nuage.

Remarque Si vous souhaitez utiliser le satellite Smart Software Manager, utilisez Smart Software Manager Satellite Enhanced Edition 6.1.0.

- Les utilisateurs existants de licences classiques (traditionnelles) doivent migrer leurs licences classiques vers des licences Smart.

  Consultez https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic.
- L'horloge système de l'appliance doit être synchronisée avec celle du CSSM. Tout écart entre l'horloge système de l'appliance et celle du CSSM entraînera l'échec des opérations de licence Smart.

Remarque Si vous avez une connexion Internet et que vous souhaitez vous connecter au CSSM par l'intermédiaire d'un proxy, vous devez utiliser le même proxy que celui configuré pour l'appliance à l'aide du menu **System Administration-> Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour).

Remarque Pour les utilisateurs virtuels, chaque fois que vous recevez un nouveau fichier PAK (nouveau ou renouvelé), générez le fichier de licence et chargez-le sur l'appliance. Après avoir chargé le fichier, vous devez convertir la clé PAK en licence Smart. En mode de licence Smart, la section des clés de fonctionnalité dans le fichier de licence sera ignorée lors du chargement du fichier et seules les informations du certificat seront utilisées.

Remarque L'appliance basculera du mode de licence Smart au mode de licence classique lorsque vous reviendrez à une version antérieure d'AsyncOS. Vous devez activer les licences Smart manuellement et demander les licences requises.

Pour activer la licence logicielle Smart pour votre appliance, vous devez procéder de la manière suivante :

	Faire ceci	Plus d'informations
Étape 1	Activez les licences logicielles Smart	Activation des licences logicielles Smart , à la page 562
Étape 2	Enregistrez l'appliance auprès de Cisco Smart Software Manager	Enregistrement de l'appliance dans Cisco Smart Software Manager , à la page 563
Étape 3	Demandez les licences (clés de fonctionnalité)	Demande de licences, à la page 565

Activation des licences logicielles Smart

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Cliquez sur **Enable Smart Software Licensing** (Activer les licences logicielles Smart).

Pour en savoir plus sur les licences logicielles Smart, cliquez sur le lien **En savoir plus sur les licences logicielles Smart**.

Étape 3 Cliquez sur **OK** après avoir lu les informations sur les licences logicielles Smart.

Étape 4 Validez vos modifications.

Prochaine étape

Après avoir activé les licences logicielles Smart, toutes les fonctionnalités du mode d'octroi de licences classique seront automatiquement disponibles dans le mode d'octroi de licences Smart. Si vous êtes un utilisateur existant en mode de licence classique, vous avez une période d'évaluation de 90 jours pour utiliser la fonctionnalité de licence logicielle Smart sans enregistrer votre appliance auprès du CSSM.

Vous recevrez des notifications à des intervalles réguliers (90e, 60e, 30e, 15e, 5e et dernier jour) avant l'expiration et aussi à l'expiration de la période d'évaluation. Vous pouvez enregistrer votre appliance auprès du CSSM pendant ou après la période d'évaluation.

Remarque

- Les nouveaux utilisateurs d'appliance virtuelle sans licence active en mode de licence classique n'auront pas de période d'évaluation même s'ils activent la fonction d'octroi de licences logicielles Smart. Seuls les utilisateurs de l'appliance virtuelle existante avec des licences actives en mode de licence classique auront une période d'évaluation. Si de nouveaux utilisateurs d'appliance virtuelle souhaitent évaluer la fonctionnalité de licences Smart, communiquez avec l'équipe des ventes de Cisco pour ajouter la licence d'évaluation au compte Smart. Les licences d'évaluation sont utilisées à des fins d'évaluation après l'enregistrement.
- Après avoir activé la fonction de licences Smart sur votre appliance, vous ne pourrez pas revenir du mode de licences Smart au mode d'octroi de licences classique.
- Les fonctionnalités suivantes sont redémarrées lorsque vous activez la fonction d'octroi de licences Smart :
  - Secure Web Appliance Filtres de réputation Web
  - Secure Web Appliance Anti-Virus Sophos
  - Secure Web Appliance Anti-Virus Webroot
  - Secure Web Appliance Proxy Web et moteur DVS
- Dans AsyncOS version 15.0, les licences Smart peuvent être activées pour les nouveaux déploiements virtuels de Cisco Secure Web Appliance. Même si la licence classique n'est pas obligatoire. Pour en savoir plus, consultez les conditions préalables disponibles dans la section Survol.

Enregistrement de l'appliance dans Cisco Smart Software Manager

Vous devez activer la fonction d'octroi de licences logicielles Smart dans le menu System Administration (Administration système) afin d'enregistrer votre appliance auprès de Cisco Smart Software Manager.

Remarque Vous ne pouvez pas enregistrer plusieurs appliances dans une seule instance. Vous devez enregistrer les appliances une par une.

Étape 1 Choisissez **System Administration** > **Smart Software Licensing** (Administration système > Licences logicielles Smart).

Étape 2 Sélectionnez l'option **Smart License Registration** (Enregistrement de licence Smart).

Étape 3 Cliquez sur **Confirm (Confirmer)**.

Étape 4 Cliquez sur **Edit** (Modifier) si vous souhaitez modifier les paramètres de transport. Les options disponibles sont les suivantes :

- **Direct** : connecte l'appliance directement à Cisco Smart Software Manager par le biais du protocole HTTP. Cette option est sélectionnée par défaut.
- **Transport Gateway** (Passerelle de transport) : connecte l'appliance à Cisco Smart Software Manager par l'intermédiaire d'une passerelle de transport ou d'un satellite Smart Software Manager. Lorsque vous choisissez cette option, vous devez entrer l'URL de la passerelle de transport ou du satellite Smart Software Manager et

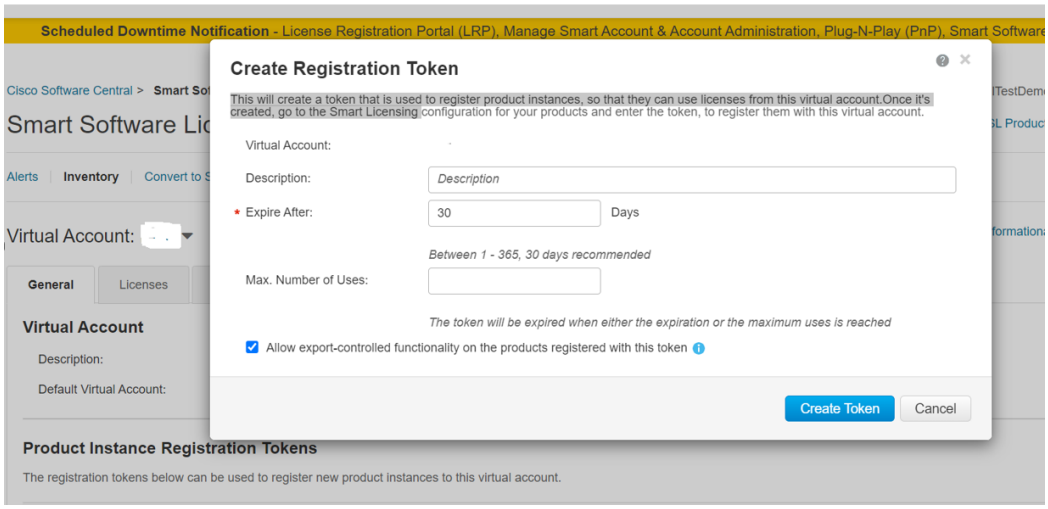
cliquer sur OK. Cette option prend en charge HTTP et HTTPS. En mode FIPS, la passerelle de transport prend en charge uniquement HTTPS.

Consultez le site https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur la passerelle de transport.

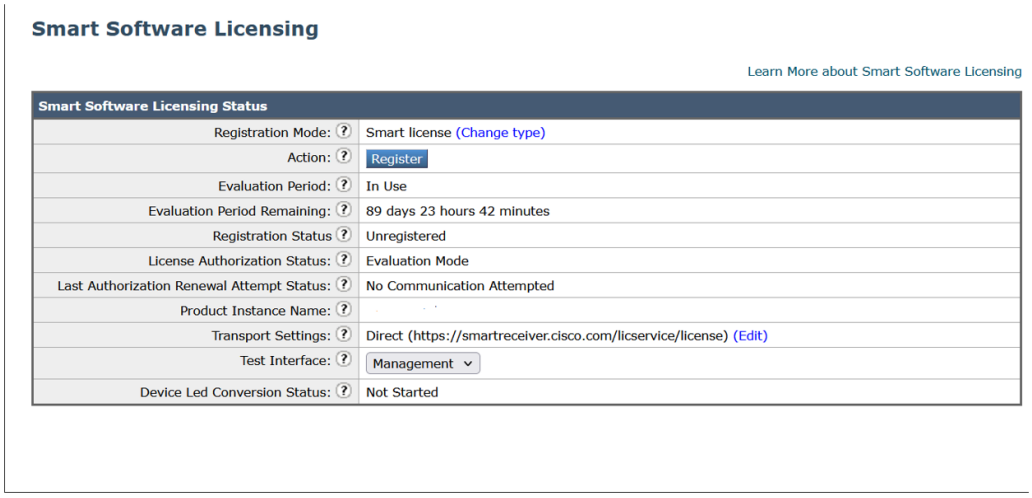
Étape 5 (Facultatif) **Tester l'interface** : choisissez l'interface de gestion ou de données lors de l'enregistrement de l'appliance pour la fonction de licence Smart. Cela s'applique uniquement lorsque vous activez le routage fractionné et que vous vous inscrivez pour obtenir une licence Smart.

Remarque Si le routage fractionné n'est pas activé, seule l'option d'interface de gestion est disponible dans la liste déroulante **Test Interface** (Tester l'interface).

Étape 6 Accédez au portail Cisco Smart Software Manager (https://software.cisco.com/#module/SmartLicensing) en utilisant vos coordonnées de connexion. Accédez à la page Virtual Account (Compte virtuel) du portail et accédez à l'onglet General (Général) pour générer un nouveau jeton. Copiez le jeton d'enregistrement d'instance de produit pour votre appliance. Consultez le site https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur la création des jetons d'enregistrement d'instance de produit.

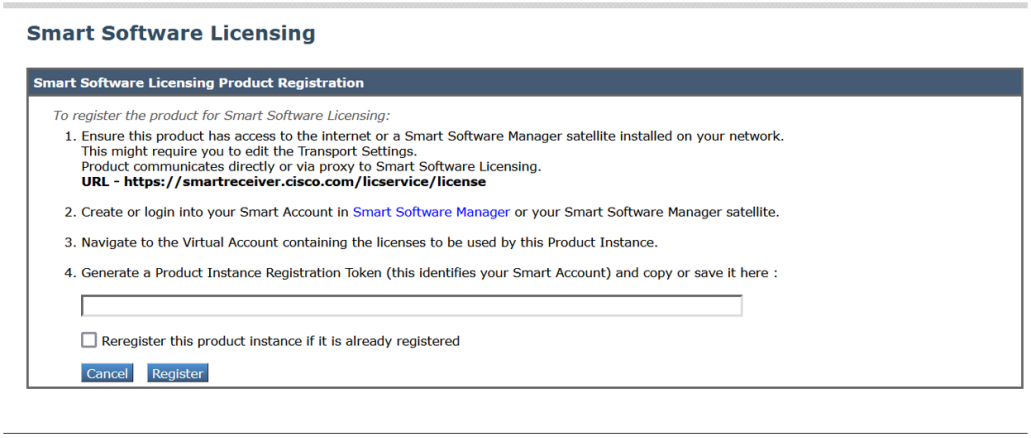


Étape 7 Revenez à votre appliance et cliquez sur **Register**(Enregistrer).



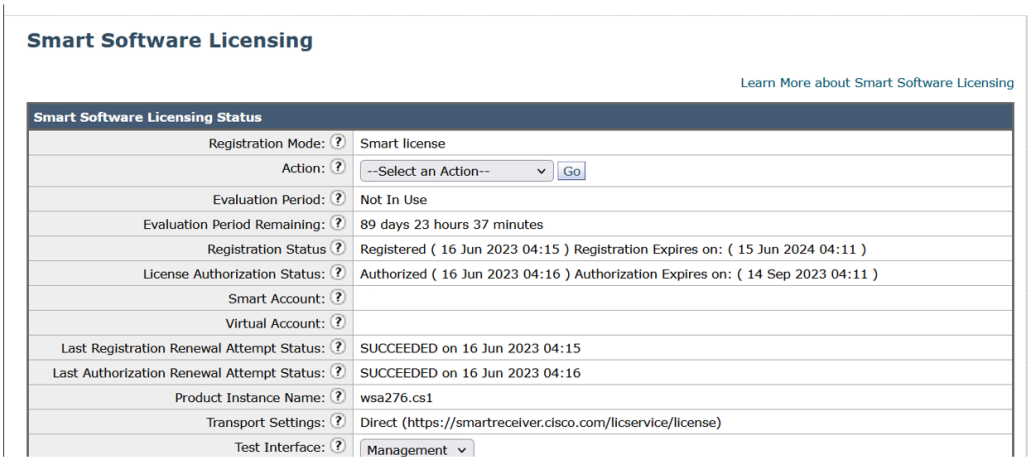
Étape 8 Collez le **jeton d'enregistrement d'instance de produit** dans la zone de texte.

Dans la page Smart Software Licensing (Licences logicielles Smart), vous pouvez cocher la case **Reregister this product instance if it is already registered** (Réenregistrer cette instance de produit si elle est déjà enregistrée) pour réenregistrer votre appliance.



Prochaine étape

Le processus d'enregistrement du produit prend quelques minutes et vous pouvez voir l'état de l'enregistrement dans la page des licences logicielles Smart.



Demande de licences

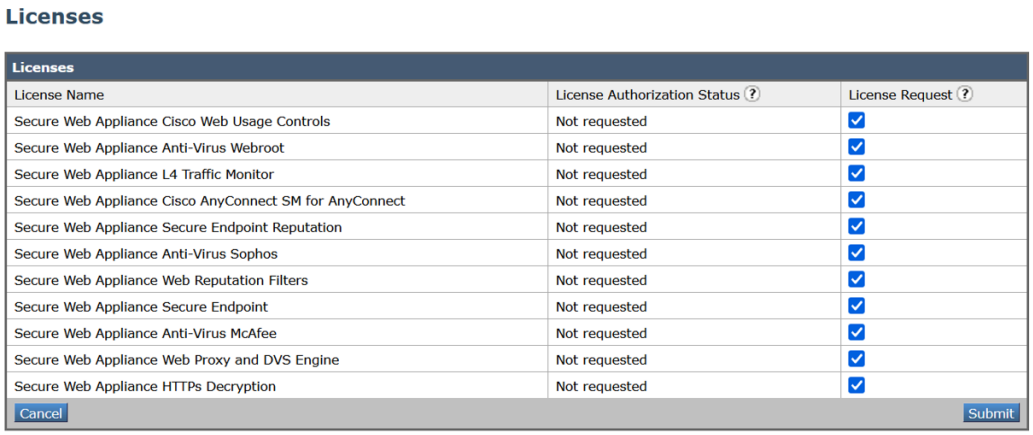
Une fois que vous avez terminé le processus d'enregistrement, vous devez demander des licences pour les fonctionnalités de l'appliance, au besoin.

Étape 1 Choisissez **System Administration > Licenses** (Administration système > Licences).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez les cases sous la colonne License Request/Release (Demande/émission de licence) correspondant aux licences que vous souhaitez demander.

Étape 4 Cliquez sur **Submit** (Soumettre).



Prochaine étape

Lorsque les licences sont utilisées excessivement ou expirent, elles passent en mode non conforme (OOC) et un délai de grâce de 30 jours est accordé pour chaque licence. Vous recevrez des notifications à des intervalles réguliers (le 30e, le 15e, le 5e et le dernier jour) avant l'expiration et à l'expiration du délai de grâce OOC.

Après l'expiration du délai de grâce OOC, vous ne pourrez plus utiliser les licences et les fonctionnalités ne seront pas disponibles. Pour accéder de nouveau aux fonctionnalités, vous devrez mettre à jour les licences sur le portail CSSM et renouveler l'autorisation.

Octroi de licences

Étape 1 Choisissez **System Administration > Licenses** (Administration système > Licences).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Décochez les cases sous la colonne License Request (Demande de licence) correspondant aux licences que vous souhaitez émettre.

Étape 4 Cliquez sur **Submit** (Soumettre).

Annulation de l'enregistrement de l'appliance dans Cisco Smart Software Manager

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la liste déroulante **Action**, choisissez **Deregister** (Annuler l'enregistrement) et cliquez sur **Go** (Aller).

Étape 3 Cliquez sur **Submit** (Soumettre).

Réenregistrement de l'appliance dans Cisco Smart Software Manager

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la liste déroulante **Action**, choisissez **Reregister** (Réenregistrer), puis cliquez sur **Go** (Aller).

Prochaine étape

Consultez Enregistrement de l'appliance dans Cisco Smart Software Manager , à la page 563 pour en savoir plus sur le processus d'enregistrement.

Vous pouvez réenregistrer l'appliance après avoir réinitialisé les configurations de l'appliance dans des scénarios inévitables.

Modification des paramètres de transport

Vous pouvez modifier les paramètres de transport uniquement avant d'enregistrer l'appliance auprès du CSSM.

Remarque Vous pouvez modifier les paramètres de transport uniquement lorsque la fonction de licence Smart est activée. Si vous avez déjà enregistré votre appliance, vous devez annuler l'enregistrement de l'appliance pour modifier les paramètres de transport. Après avoir modifié les paramètres de transport, vous devez enregistrer à nouveau l'appliance.

Consultez Enregistrement de l'appliance dans Cisco Smart Software Manager , à la page 563 pour savoir comment modifier les paramètres de transport.

Renouvellement de l'autorisation et du certificat

Après avoir enregistré votre appliance auprès de Smart Cisco Software Manager, vous pouvez renouveler le certificat.

Remarque Vous ne pouvez renouveler l'autorisation qu'après l'enregistrement réussi de l'appliance.

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la liste déroulante **Action**, choisissez l'option appropriée :

- **Renew Authorization Now** (Renouveler l'autorisation maintenant)
- **Renew Certificates Now** (Renouveler le certificat maintenant)

Étape 3 Cliquez sur **Go** (Aller).

Prochaine étape

Mise à jour de Smart Agent

Pour mettre à jour la version de Smart Agent installée sur votre appliance, procédez comme suit :

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la section **Smart Agent Update Status** (État de mise à jour de Smart Agent), cliquez sur **Update Now** (Mettre à jour maintenant) et suivez la procédure.

Remarque Si vous essayez d'enregistrer des modifications de configuration à l'aide de la commande `saveconfig` de l'interface de ligne de commande ou à l'aide de l'interface Web, en sélectionnant **System Administration > Configuration Summary** (Administration système > Résumé de la configuration), la configuration liée aux licences Smart ne sera pas enregistrée.

Alerts (Alertes)

Vous recevrez des notifications dans les scénarios suivants :

- Licence logicielle Smart activée avec succès
- Échec de l'activation de l'octroi de licences logicielles Smart
- Début de la période d'évaluation
- Expiration de la période d'évaluation (à des intervalles réguliers pendant la période d'évaluation et à l'expiration)
- Enregistrement réussi
- Échec de l'enregistrement
- Autorisation réussie
- Échec de l'autorisation
- Désenregistrement réussi
- Échec du désenregistrement
- Certificat d'ID renouvelé avec succès
- Échec du renouvellement du certificat d'ID
- Expiration de l'autorisation
- Expiration du certificat d'ID
- Expiration du délai de grâce de non-conformité (à des intervalles réguliers pendant le délai de grâce et à l'expiration).
- Première instance de l'expiration d'une fonctionnalité

Interface de commande en ligne

license_smart

Description

Configurez la fonction d'octroi de licences logicielles intelligentes.

Utilisation

Commit (Valider) : cette commande nécessite une « validation ».

Batch Command (Commande par lot) : cette commande prend en charge le format par lot. Pour en savoir plus, consultez l'aide en ligne en saisissant la commande : `Help license_smart`.

Exemple : configuration du port pour le service Smart Agent

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

Exemple : activation des licences Smart

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
 []> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):
```

```
a) Register the product with Smart Software Manager using license_smart > register command
 in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
 period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
 [Y/N] []> y

> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

Exemple : enregistrement de l'appliance dans Smart Software Manager

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx
OXhuenN4OWZDdktFckJLQzF5V3VIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
 registration.
```

Exemple : état des licences Smart

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode
```

```
Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Exemple : résumé de l'état des licences Smart

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary

FeatureName                                  LicenseAuthorizationStatus
Web Security Appliance Cisco                 Eval
Web Usage Controls
Web Security Appliance Anti-Virus Webroot    Eval
Web Security Appliance Anti-Virus Sophos     Eval
```

Exemple : Définition de l'URL de Smart Transport

```
example.com> license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url

1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager
 satellite.

Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig command.
Transport settings will be updated after commit.
```

Exemple : demande de licences

Remarque Les utilisateurs d'appliances virtuelles doivent enregistrer leur appliance pour demander ou émettre les licences.

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
```

```
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                    License Authorization Status
1. Web Security Appliance Anti-Virus Sophos      Not Requested
2. Web Security Appliance                        Not requested
   L4 Traffic Monitor

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Web Security Appliance Anti-Virus Sophos
Use license_smart > summary command to check status of licenses.
```

Exemple : octroi de licences

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license

Feature Name                                  License Authorization Status
1. Web Security Appliance Cisco               Eval
   Web Usage Controls
2. Web Security Appliance                     Eval
   Anti-Virus Webroot
3. Web Security Appliance                     Eval
   L4 Traffic Monitor
4. Web Security Appliance Cisco               Eval
   AnyConnect SM for AnyConnect
5. Web Security Appliance Advanced            Eval
   Malware Protection Reputation
6. Web Security Appliance                     Eval
   Anti-Virus Sophos
7. Web Security Appliance                     Eval
   Web Reputation Filters
8. Web Security Appliance Advanced            Eval
   Malware Protection
```

show_license

- Description, à la page 572
- Exemple : état des licences Smart, à la page 573
- Exemple : résumé de l'état des licences Smart, à la page 573

Description

Affichez l'état des licences Smart et un résumé de l'état.

Exemple : état des licences Smart

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Exemple : résumé de l'état des licences Smart

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary

FeatureName                          LicenseAuthorizationStatus
Web Security Appliance Cisco         Eval
Web Usage Controls
Web Security Appliance               Eval
Anti-Virus Webroot
Web Security Appliance               Eval
Anti-Virus Sophos
```

cloudserviceconfig

Description

La commande **cloudserviceconfig** est utilisée pour :

- Activer le portail des services Cisco Cloud sur Secure Web Appliance.
- Désactiver le portail des services Cisco Cloud sur Secure Web Appliance.
- Enregistrer votre Secure Web Appliance sur le portail des services Cisco Cloud.
- Enregistrer automatiquement votre Secure Web Appliance sur le portail des services Cisco Cloud.
- Annuler l'enregistrement de votre Secure Web Appliance sur le portail des services Cisco Cloud.
- Choisissez le serveur Cisco Secure Cloud pour connecter Secure Web Appliance au portail des services Cisco Cloud.
- Téléchargez le certificat et la clé de services Cisco Cloud à partir du portail des services Cisco Talos Intelligence.
- Chargement du certificat client et de la clé

Remarque Cette commande est applicable uniquement en mode de licences Smart.

Utilisation

- **Commit** (Valider) : cette commande ne nécessite pas de « validation ».
- **Batch Command** (Commande par lot) : cette commande prend en charge le format par lot.

Exemple : activation des services Cisco Cloud sur Secure Web Appliance

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > enable` pour activer les services Cisco Cloud sur Secure Web Appliance

```
example.com > cloudserviceconfig
Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
[]> enable
The Cisco Cloud Service is currently enabled on your appliance.
Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 1
Selected Cisco Secure Cloud Server is api-sse.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:23:19 2020 GMTexample.com >
```

Exemple : désactivation des services Cisco Cloud sur Secure Web Appliance

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > disable` pour désactiver les services Cisco Cloud sur Secure Web Appliance.

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
```

```
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> disable
The Cisco Cloud Service is currently disabled on your appliance.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:01:07 2020 GMT
example.com >
```

Exemple : enregistrement de Secure Web Appliance sur le portail des services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > register` pour enregistrer Secure Web Appliance sur le portail des services Cisco Cloud.

Remarque Vous ne pouvez utiliser cette sous-commande que si l'octroi de licences logicielles Smart n'est pas activé et que Secure Web Appliance n'est pas enregistré dans Cisco Smart Software Manager

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> register

Enter a registration token key to register your appliance
[]> c51fa32bd9a31227eaab50dea873062c

Registering
The Web Security appliance is successfully registered with the Cisco Cloud Service portal.
example.com >
```

Exemple : enregistrement automatique de Secure Web Appliance sur le portail des services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la commande `cloudserviceconfig > autoregister` pour enregistrer Secure Web Appliance auprès du portail des services Cisco Cloud.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically
using SL Payload.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> autoregister

The Web Security appliance successfully auto-registered with the Cisco Cloud Service portal.
```

Exemple : Désenregistrement de Secure Web Appliance du portail de services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig` > `deregister` pour annuler l'enregistrement de Secure Web Appliance auprès du portail des services Cisco Cloud.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> deregister

Do you want to deregister your appliance from the Cisco Cloud Service portal.
If you deregister, you will not be able to access the Cloud Service features. [N]> y

The Web Security appliance successfully deregistered from the Cisco Cloud Service portal.
example.com >
```

Exemple : choix du serveur Cisco Secure Cloud pour connecter Secure Web Appliance au portail des services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig` > `settrs` pour choisir le serveur Cisco Secure Cloud requis pour connecter Secure Web Appliance au portail des services Cisco Cloud.

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> settrs
Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 3
Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:37:40 2020 GMT
```

Exemple : téléchargement du certificat et de la clé pour les services Cisco Cloud à partir du portail de services de renseignement Cisco Talos

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig` > `fetchcertificate` pour télécharger le certificat et la clé des services Cisco Cloud à partir du portail des services Cisco Talos Intelligence.

Remarque Vous ne pouvez utiliser cette sous-commande que lorsque le certificat des services Cisco Cloud existant a expiré et si vous avez enregistré Secure Web Appliance avec Cisco Smart Software Manager.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:


Choose the operation you want to perform:
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> fetchcertificate

Successfully downloaded the Cisco Talos certificate and key
example.com >
```

Exemple : certificat client (updateconfig)

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `Updateconfig > clientcertificate` pour charger le certificat et la clé.

```
example.com > updateconfig

Service (images):                   Update URL:
------------------------------------------------------------------------------
Web Reputation Filters              Cisco Servers
Support Request updates             Cisco Servers
Timezone rules                      Cisco Servers
How-Tos Updates                     Cisco Servers
HTTPS Proxy Certificate Lists       Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers
Smart License Agent Updates         Cisco Servers

Service (list):                     Update URL:
------------------------------------------------------------------------------
Web Reputation Filters              Cisco Servers
Support Request updates             Cisco Servers
Timezone rules                      Cisco Servers
How-Tos Updates                     Cisco Servers
HTTPS Proxy Certificate Lists       Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers
Smart License Agent Updates         Cisco Servers

Update interval for Web Reputation and Categorization: 5m
Update interval for all other services: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
    The following services will use this routing table:
    - Web Reputation Filters
    - Support Request updates
    - Timezone rules
    - How-Tos Updates
    - HTTPS Proxy Certificate Lists
    - Cisco AsyncOS upgrades
    - Smart License Agent Updates

Upgrade notification: enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> clientcertificate
```

```
Current Cisco certificate is valid for 179 days

Do you like to overwrite the existing certificate and key [Y|N] ? []> y

Paste the certificate.
Press CTRL-D on a blank line when done.
^D
```

Collez les détails de votre certificat et de votre clé privée. Le certificat et la clé sont stockés avec succès.

Smart Software Licensing Points pour AsyncOS 14.0 et versions ultérieures

- Lorsque l'octroi de licences logicielles Smart est activé et enregistré, le service Cisco Cloud est activé et enregistré automatiquement.
- Si le certificat des services Cisco Cloud a expiré, vous pouvez maintenant télécharger un nouveau certificat à partir du portail des services Cisco Talos Intelligence à l'aide de la sous-commande `cloudserviceconfig > fetchcertificate` de l'interface de ligne de commande.
- Vous ne pouvez pas effectuer l'enregistrement automatique auprès du service Cisco Cloud lorsque la licence Smart est en mode d'évaluation.

Licence pour appliance virtuelle

L'appliance virtuelle Cisco Web Security nécessite une licence supplémentaire pour l'exécuter sur un hôte.

Pour en savoir plus sur les licences d'appliances virtuelles, consultez le *Guide d'installation de Cisco Content Security Virtual Appliance*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Note Vous ne pouvez pas ouvrir un tunnel d'assistance technique avant d'installer la licence d'appliance virtuelle.

Après l'expiration de la licence, l'appliance continue de servir de proxy Web sans services de sécurité pendant 180 jours. Aucune mise à jour des services de sécurité n'est effectuée pendant cette période.

Vous pouvez configurer l'appliance de manière à recevoir des alertes concernant l'expiration de la licence.

Thèmes connexes

- Gestion des alertes, on page 590

Installation d'une licence d'appliance virtuelle

Voir le *Guide d'installation de Cisco Content Security Virtual Appliance*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Activation du redémarrage à distance

Before you begin

- Câblez le port dédié au redémarrage à distance (RPC) directement à un réseau sécurisé. Pour plus d'informations, consultez le guide du matériel pour votre modèle d'appliance. Pour connaître l'emplacement de ce document, consultez Documentation, on page 695.
- Vérifiez que l'appliance est accessible à distance; par exemple, ouvrez tous les ports nécessaires sur le pare-feu.
- Cette fonction nécessite une adresse IPv4 unique pour l'interface dédiée au redémarrage à distance. Cette interface ne peut être configurée qu'au moyen de la procédure décrite dans cette section; elle ne peut pas être configurée à l'aide de la commande ipconfig.
- Pour redémarrer l'appliance, vous aurez besoin d'un outil tiers capable de gérer les périphériques qui prennent en charge Intelligent Platform Management Interface (IPMI) version 2.0. Assurez-vous d'être prêt à utiliser un tel outil.
- Pour en savoir plus sur l'accès à l'interface de ligne de commande, consultez Interface de commande en ligne, on page 667

Après avoir configuré la fonction RPC et validé les modifications, attendez 10 à 15 minutes avant d'envoyer les appels à RPC. Secure Web Appliance initialise les services RCP pendant ce temps d'attente.

La possibilité de réinitialiser l'alimentation à distance pour le châssis de l'appliance est disponible sur le matériel séries x80, x90 et x95.

Si vous souhaitez pouvoir redémarrer à distance l'appliance, vous devez activer et configurer cette fonctionnalité au préalable, en utilisant la procédure décrite dans cette section.

Étape 1 Utilisez SSH ou le port de console série pour accéder à l'interface de ligne de commande.

Étape 2 Connectez-vous en utilisant un compte avec accès administrateur.

Étape 3 Saisissez les commandes suivantes :

```
remotepower

Configurer
```

Étape 4 Suivez les invites pour définir les éléments suivants :

- Adresse IP dédiée à cette fonctionnalité, plus le masque réseau et la passerelle.
- Le nom d'utilisateur et la phrase secrète nécessaires pour exécuter la commande de redémarrage.

  Ces informations d'authentification sont indépendantes des autres informations d'authentification utilisées pour accéder à votre appliance.

Étape 5 Saisissez `commit` (valider) pour enregistrer vos modifications.

Étape 6 Testez votre configuration pour vous assurer que vous pouvez gérer l'alimentation de l'appliance à distance.

Étape 7 Assurez-vous que les identifiants que vous avez saisis seront disponibles indéfiniment. Par exemple, rangez ces informations en lieu sûr et assurez-vous que les administrateurs qui peuvent avoir besoin d'effectuer cette tâche ont accès aux informations d'authentification requises.

What to do next

Thèmes connexes

- Appliances matérielles : réinitialisation à distance de l'alimentation des appliances , on page 658

Administration des comptes d'utilisateur

Les types d'utilisateurs suivants peuvent se connecter à l'appliance pour la gérer :

- **Utilisateurs locaux.** Vous pouvez définir les utilisateurs localement, sur l'appliance même.
- **Utilisateurs définis dans un système externe.** Vous pouvez configurer l'appliance de sorte qu'elle se connecte à un serveur LDAP ou RADIUS externe pour authentifier les utilisateurs qui se connectent à l'appliance.

Note Tout utilisateur que vous définissez peut se connecter à l'appliance par n'importe quelle méthode, par exemple par la connexion à l'interface Web ou par SSH.

Thèmes connexes

- Gestion des comptes d'utilisateur locaux, on page 580
- Authentification des utilisateurs RADIUS, on page 583
- Configuration de l'authentification extérieure par l'intermédiaire d'un serveur LDAP, on page 116

Gestion des comptes d'utilisateur locaux

Vous pouvez définir n'importe quel nombre d'utilisateurs localement sur Secure Web Appliance.

Le compte d'administrateur système par défaut dispose de tous les privilèges d'administration. Vous pouvez modifier la phrase secrète du compte administrateur, mais vous ne pouvez pas modifier ou supprimer ce compte.

Note Si vous avez perdu la phrase secrète de l'utilisateur admin, communiquez avec votre fournisseur d'assistance Cisco. Pour en savoir plus, consultez Réinitialiser votre mot de passe administrateur et déverrouiller le compte utilisateur administrateur.

Ajout de comptes d'utilisateur locaux

Before you begin

Définissez les exigences relatives à la phrase secrète que tous les comptes d'utilisateur doivent respecter. Consultez Définition des exigences de phrase secrète pour les utilisateurs administratifs , on page 586.

Étape 1 Choisissez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Cliquez sur **Add User** (Ajouter un utilisateur).

Étape 3 Saisissez un nom d'utilisateur en respectant les règles suivantes :

- Les noms d'utilisateur peuvent contenir des lettres minuscules, des chiffres et le tiret (-), mais ne peuvent pas commencer par un tiret.
- Les noms d'utilisateur ne peuvent pas dépasser 16 caractères.
- Les noms d'utilisateur ne peuvent pas être des noms spéciaux réservés par le système, comme « operator » ou « root ».
- Si vous utilisez également l'authentification extérieure, les noms d'utilisateurs ne doivent pas dupliquer des noms d'utilisateurs authentifiés en externe.

Étape 4 Saisissez le nom complet de l'utilisateur.

Étape 5 Sélectionnez un type d'utilisateur

Type d'utilisateur	Description
Administrateur	Autorise l'accès complet à tous les paramètres de configuration du système. Cependant, les commandes de l'interface de ligne de commande `upgradecheck` et `upgradeinstall` ne peuvent être exécutées qu'à partir du compte « admin » défini par le système.
Opérateur	Empêche les utilisateurs de créer, de modifier ou de supprimer des comptes d'utilisateur. Le groupe Opérateurs restreint également l'utilisation des commandes suivantes de l'interface de ligne de commande : • `resetconfig` • `upgradecheck` • `upgradeinstall` Le groupe des opérateurs restreint également l'utilisation de l'Assistant de configuration du système.

Type d'utilisateur	Description
Opérateur en lecture seule	Les comptes utilisateur possédant ce rôle : • Peuvent afficher les informations de configuration. • Peuvent effectuer et envoyer des modifications pour voir comment configurer une fonctionnalité, mais ne peuvent pas les valider. • Ne peuvent pas apporter d'autres modifications à l'appliance, comme effacer le cache ou enregistrer des fichiers. • Ne peuvent pas accéder au système de fichiers, au FTP ou au SCP.
Invité	Les utilisateurs du groupe des invités peuvent uniquement afficher les informations sur l'état du système, y compris les rapports et le suivi.

Étape 6 Saisissez ou générez une phrase secrète.

Étape 7 Envoyez et validez vos modifications.

Suppression de comptes d'utilisateur

Étape 1 Choisissez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Cliquez sur l'icône de la corbeille correspondant au nom d'utilisateur indiqué et confirmez lorsque vous y êtes invité.

Étape 3 Envoyez et validez vos modifications.

Modifications de comptes d'utilisateur

Étape 1 Choisissez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Cliquez sur le nom d'utilisateur.

Étape 3 Apportez les modifications nécessaires à l'utilisateur sur la page Edit User (Modifier l'utilisateur).

Étape 4 Envoyez et validez vos modifications.

Modification des phrases secrètes

Pour modifier la phrase secrète du compte actuellement connecté, sélectionnez **Options > Change Passphrase** (Options > Modifier la phrase secrète) dans le coin supérieur droit de la fenêtre.

Pour les autres comptes, modifiez le compte et la phrase secrète dans la page Local User Settings (Paramètres de l'utilisateur local).

Thèmes connexes

- Modifications de comptes d'utilisateur, on page 582

• Définition des exigences de phrase secrète pour les utilisateurs administratifs , on page 586

Configuration de paramètres restrictifs de comptes d'utilisateur et de phrases secrètes

Vous pouvez définir des restrictions de compte d'utilisateur et de phrase secrète pour appliquer les politiques de phrase secrète de l'entreprise. Les restrictions liées au compte d'utilisateur et à la phrase secrète s'appliquent aux utilisateurs locaux définis sur l'appliance Cisco. Vous pouvez configurer les paramètres suivants :

- **Verrouillage du compte d'utilisateur.** Vous pouvez définir le nombre de tentatives de connexion infructueuses entraînant le blocage de l'accès du compte à l'utilisateur. Vous pouvez définir le nombre de tentatives de connexion de l'utilisateur entre 1 et 60. La valeur par défaut est égale à 5.
- **Règles relatives à la durée de vie des phrases secrètes.** Vous pouvez définir la durée de vie d'une phrase secrète avant que l'utilisateur ne soit tenu de la modifier après s'être connecté.
- **Règles relatives aux phrases secrètes.** Vous pouvez définir les types de phrase secrète que les utilisateurs peuvent choisir, par exemple les caractères facultatifs ou obligatoires.

Remarque À partir de la version 14.0 d'AsyncOS, les règles de phrase secrète sont activées par défaut, à l'exception du **refus de 3 caractères répétitifs ou séquences supérieurs dans les phrases secrètes** et **de la liste de mots à interdire dans les règles de phrase secrète**.

- **Force des phrases secrètes.** Vous pouvez afficher un indicateur de force de phrase secrète lorsqu'un utilisateur administrateur saisit une nouvelle phrase secrète.

  Pour en savoir plus, consultez Définition des exigences de phrase secrète pour les utilisateurs administratifs .

Vous définissez les restrictions de compte d'utilisateur et de phrase secrète sur la page System Administration > Users (Administration système > Utilisateurs) dans la section Local User Account and Passphse Settings (Paramètres de compte d'utilisateur local et de phrase secrète).

Authentification des utilisateurs RADIUS

Secure Web Appliance peut utiliser un service d'annuaire RADIUS pour authentifier les utilisateurs qui se connectent à l'appliance à l'aide de HTTP, HTTPS, SSH et FTP. Vous pouvez configurer l'appliance pour contacter plusieurs serveurs externes aux fins d'authentification, en utilisant l'authentification PAP ou CHAP. Vous pouvez mapper des groupes d'utilisateurs externes sur différents types de rôles utilisateur Secure Web Appliance.

Séquence des événements pour l'authentification Radius

Lorsque l'authentification extérieure est activée et qu'un utilisateur se connecte à Secure Web Appliance, l'appliance :

1. Détermine si l'utilisateur est le compte « admin » défini par le système.
2. Sinon, vérifie le premier serveur externe configuré pour déterminer si l'utilisateur y est défini.
3. Si l'appliance ne peut pas se connecter au premier serveur externe, elle vérifie le serveur externe suivant dans la liste.

4. Si l'appliance ne peut pas se connecter à un serveur externe, elle tente d'authentifier l'utilisateur en tant qu'utilisateur local, défini sur la Secure Web Appliance.
5. Si l'utilisateur n'existe sur aucun serveur externe ou sur l'appliance, ou si l'utilisateur saisit la mauvaise phrase secrète, l'accès à l'appliance est refusé.

Activation de l'authentification extérieure à l'aide de RADIUS

Étape 1 Dans la page **System Administration > Users** (Administration système > Utilisateurs), cliquez sur **Enable External Authentication** (Activer l'authentification extérieure).

Étape 2 Choisissez **RADIUS** dans le champ Authentication Type (Type d'authentification).

Étape 3 Saisissez le nom d'hôte, le numéro de port et la phrase secrète du secret partagé pour le serveur RADIUS. Le port par défaut est `1812`.

Étape 4 Saisissez le nombre de secondes pendant lesquelles l'appliance doit attendre une réponse du serveur avant d'expirer.

Étape 5 Choisissez le protocole d'authentification utilisé par le serveur RADIUS.

Étape 6 (Facultatif) Cliquez sur **Add Row** (Ajouter une ligne) pour ajouter un autre serveur RADIUS. Répétez les **étapes 1 à 5** pour chaque serveur RADIUS.

Note Vous pouvez ajouter jusqu'à dix serveurs RADIUS.

Étape 7 Dans le champ **External Authentication Cache Timeout** (Délai d'expiration du cache d'authentification extérieure), saisissez le nombre de secondes pendant lesquelles AsyncOS stocke les informations d'authentification extérieure avant de recontacter le serveur RADIUS pour s'authentifier à nouveau. La valeur par défaut est zéro.

Note Si le serveur RADIUS utilise des phrases secrètes à usage unique, par exemple des phrase secrètes créées à partir d'un jeton, saisissez zéro (0). Lorsque la valeur est définie sur zéro, AsyncOS ne contacte pas à nouveau le serveur RADIUS pour s'authentifier pendant la session en cours.

Étape 8 Configure Group Mapping (Configuration du mappage de groupe) : sélectionnez s'il faut mapper tous les utilisateurs authentifiés en externe sur le rôle administrateur ou sur différents types de rôles utilisateur de l'appliance.

Paramètres	Description
Map externally authenticated users to multiple local roles (Mapper les utilisateurs authentifiés de l'extérieur sur plusieurs rôles locaux)	Saisissez un nom de groupe tel que défini dans l'attribut RADIUS CLASS et choisissez un type de rôle pour l'appliance. Vous pouvez ajouter d'autres mappages de rôles en cliquant sur Ajouter une ligne. AsyncOS affecte les utilisateurs RADIUS aux rôles dans l'appliance en fonction de l'attribut CLASS de RADIUS. Exigences de l'attribut CLASS : • au moins trois caractères • 253 caractères maximum • Pas de deux-points, de virgules ni de caractères de nouvelle ligne • Un ou plusieurs attributs CLASS mappés pour chaque utilisateur RADIUS (avec ce paramètre, AsyncOS refuse l'accès aux utilisateurs RADIUS sans attribut CLASS mappé.) Si les utilisateurs RADIUS ont plusieurs attributs CLASS, AsyncOS attribue le rôle le plus restrictif. Par exemple, si un utilisateur RADIUS a deux attributs CLASS, qui sont mappés sur les rôles Opérateur et Opérateur en lecture seule, AsyncOS affecte l'utilisateur RADIUS au rôle Opérateur en lecture seule, qui est plus restrictif que le rôle Opérateur. Voici les rôles de l'appliance, classés du plus restrictif au moins restrictif : • Administrateur • Opérateur • Opérateur en lecture seule • Invité
Map all externally authenticated users to the Administrator role (Mapper tous les utilisateurs authentifiés en externe sur le rôle administrateur).	AsyncOS affecte à tous les utilisateurs RADIUS le rôle administrateur.

Étape 9 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Authentification extérieure, on page 116
- Ajout de comptes d'utilisateur locaux, on page 581.

Définition des préférences des utilisateurs

Les paramètres de préférences, tels que les formats d'affichage des rapports, sont stockés pour chaque utilisateur et sont identiques, quel que soit l'ordinateur client à partir duquel l'utilisateur se connecte à l'appliance.

Étape 1 Choisissez **Options > Preferences** (Options > Préférences).

Étape 2 Dans la page User Preferences (Préférences de l'utilisateur), cliquez sur **Edit Preferences** (Modifier les préférences).

Étape 3 Configurez les paramètres de préférences selon vos besoins.

Paramètre de préférence	Description
Language Display (Langue d'affichage)	Langue utilisée par AsyncOS pour le Web dans l'interface Web et l'interface de ligne de commande.
Landing Page (Page de destination)	Page qui s'affiche lorsque l'utilisateur se connecte à l'appliance.
Reporting Time Range Displayed (Affichage de la plage de temps des rapports) (valeur par défaut)	La plage de temps par défaut qui s'affiche pour les rapports sous l'onglet Reporting (Rapports).
Number of Reporting Rows Displayed (Nombre de lignes de rapport affichées)	Le nombre de lignes de données affichées par défaut pour chaque rapport.

Étape 4 Envoyez et validez vos modifications.

Configuration des paramètres d'administrateur

Définition des exigences de phrase secrète pour les utilisateurs administratifs

Pour définir les exigences de phrase secrète pour les utilisateurs administratifs de l'appliance définis localement :

Étape 1 Sélectionnez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Dans la section **Passphrase Settings** (Paramètres de la phrase secrète), cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Choisissez les options :

Option	Description
List of words to disallow in passphrases (Liste de mots à interdire dans les phrases secrètes)	Créez un fichier.txt avec chaque mot interdit sur une ligne distincte, puis sélectionnez le fichier pour le charger. Les téléchargements suivants remplacent les téléchargements précédents.

Option	Description
Passphrase Strength (Force des phrases secrètes)	Vous pouvez afficher un indicateur de force de phrase secrète lorsqu'un utilisateur administrateur saisit une nouvelle phrase secrète. Ce paramètre n'applique pas la création de phrase secrète sécurisée, il montre simplement à quel point il est facile de deviner la phrase secrète saisie. Sélectionnez les rôles pour lesquels vous souhaitez afficher l'indicateur. Pour chaque rôle sélectionné, entrez ensuite une valeur supérieure à zéro. Un nombre élevé signifie qu'une phrase secrète enregistrée comme forte est plus difficile à deviner. Ce paramètre n'a pas de valeur maximale, mais un nombre très élevé rend impossible la saisie d'une phrase secrète jugée « bonne ». Faites des essais pour voir quel nombre correspond le mieux à vos besoins. La force de la phrase secrète est mesurée sur une échelle logarithmique. L'évaluation est basée sur les règles d'entropie du National Institue of Standards and Technology des États-Unis, comme défini dans la norme NIST SP 800-63, section Troubleshooting. En général, les phrases secrètes sont plus strictes : • Elles sont longues. • Elles sont composées de majuscules, de minuscules, de chiffres et de caractères spéciaux. • Elles ne comprennent pas de mots figurant dans un dictionnaire, quelle que soit la langue. Pour appliquer des phrases secrètes ayant ces caractéristiques, utilisez les autres paramètres sur cette page.

Étape 4 Envoyez et validez vos modifications.

Paramètres de sécurité supplémentaires pour l'accès à l'appliance

Vous pouvez utiliser la commande `adminaccessconfig` de l'interface de ligne de commande pour configurer Secure Web Appliance afin d'avoir des exigences d'accès plus strictes pour les administrateurs qui se connectent à l'appliance.

Commande	Description
`adminaccessconfig > banner`	Configure l'appliance pour afficher le texte que vous spécifiez lorsqu'un administrateur tente de se connecter. La bannière de connexion personnalisée s'affiche lorsqu'un administrateur accède à l'appliance par une interface; par exemple, par l'interface utilisateur Web, l'interface de ligne de commande ou le FTP. Vous pouvez charger le texte personnalisé en le copiant dans l'invite de l'interface de ligne de commande ou en le copiant à partir d'un fichier texte situé sur Secure Web Appliance. Pour charger le texte à partir d'un fichier, vous devez d'abord transférer le fichier vers le répertoire de configuration de l'appliance à l'aide du protocole FTP.
`adminaccessconfig > welcome`	Il s'agit d'une bannière après la connexion, qui s'affiche après une connexion réussie de l'administrateur. Ce texte est ajouté à la configuration de l'appliance par les mêmes moyens que le texte de connexion `adminaccessconfig > banner`.
`adminaccessconfig > ipaccess`	Contrôle les adresses IP des administrateurs pour accéder à Secure Web Appliance. Les administrateurs peuvent accéder à l'appliance à partir de n'importe quelle ordinateur ou à partir d'ordinateurs dotés d'une adresse IP figurant dans une liste que vous définissez. Lorsque vous restreignez l'accès à une liste d'autorisation, vous pouvez spécifier des adresses IP, des sous-réseaux ou des adresses CIDR. Par défaut, lorsque vous répertoriez les adresses qui peuvent accéder à l'appliance, l'adresse IP de votre appliance actuelle est répertoriée comme première adresse dans la liste d'autorisation. Vous ne pouvez pas supprimer l'adresse IP de votre appliance actuelle de la liste d'autorisation. Ces informations peuvent également être fournies à l'aide de l'interface utilisateur Web; voir Accès au réseau de l'utilisateur, on page 589.
`adminaccessconfig - csrf`	Activez/désactivez la protection contre la falsification des demandes intersites de l'interface utilisateur Web, utilisée pour identifier et protéger contre les demandes malveillantes ou frauduleuses. Pour une sécurité optimale, il est recommandé d'activer la protection CSRF.
`adminaccessconfig > hostheader`	Configurez l'utilisation de l'en-tête host dans les demandes HTTP. Par défaut, l'interface utilisateur Web répond par l'en-tête d'hôte envoyé par le client Web dans une requête HTTP. Pour une sécurité accrue, vous pouvez configurer l'interface utilisateur Web de manière à répondre uniquement par le nom d'hôte propre à l'appliance, c'est-à-dire le nom configuré de l'appliance (par exemple, `wsa_04.local`).
`adminaccessconfig > timeout`	Indiquez un intervalle d'expiration de délai d'inactivité; c'est-à-dire le nombre de minutes pendant lesquelles les utilisateurs peuvent être inactifs avant d'être déconnectés. Cette valeur peut être comprise entre 5 et 1 440 minutes (24 heures). La valeur par défaut est de 30 minutes. Ces informations peuvent également être fournies à l'aide de l'interface utilisateur Web; voir Accès au réseau de l'utilisateur, on page 589.

Commande	Description
`adminaccessconfig > how-tos`	Activez des procédures pas à pas qui vous aident à accomplir des tâches de configuration spécifiques.
`adminaccessconfig > strictssl`	Configure l'appliance pour que les administrateurs se connectent à l'interface Web sur le port 8443 à l'aide de chiffrements SSL plus forts (chiffrement supérieur à 56 bits). Lorsque vous configurez l'appliance pour exiger des chiffrements SSL plus forts, la modification s'applique uniquement aux administrateurs accédant à l'appliance à l'aide du protocole HTTPS pour gérer l'appliance. Elle ne s'applique pas aux autres trafics réseau connectés au proxy Web à l'aide de HTTPS.
`adminaccessconfig > loginhistory`	Configurez le nombre de jours pendant lesquels l'historique de connexion est conservé.
`adminaccessconfig > maxsessions`	Configurez le nombre maximal de sessions de connexion simultanées (CLI et interface Web).

Accès au réseau de l'utilisateur

Vous pouvez spécifier combien de temps un utilisateur peut être connecté à l'appliance avant qu'AsyncOS ne déconnecte l'utilisateur pour cause d'inactivité. Vous pouvez également indiquer le type de connexions utilisateur autorisées.

L'expiration de la session s'applique à tous les utilisateurs, y compris les administrateurs, connectés à l'interface utilisateur Web ou à l'interface de ligne de commande. Si AsyncOS déconnecte un utilisateur, celui-ci est redirigé vers la page de connexion de l'appliance.

Remarque Vous pouvez également utiliser l'interface de ligne de commande `adminaccessconfig > timeout` pour définir cette valeur d'expiration.

Étape 1 Choisissez **System Administration** > **Network Access** (Administration système > Accès au réseau).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans le champ **Session Inactivity Timeout** (Délai d'expiration pour inactivité de session), saisissez le nombre de minutes que les utilisateurs peuvent être inactifs avant d'être déconnectés.

Vous pouvez définir un intervalle d'expiration entre cinq et 1 440 minutes (24 heures); la valeur par défaut est 30 minutes.

Étape 4 Dans la section **User Access** (Accès de l'utilisateur), vous contrôlez l'accès au système des utilisateurs : choisissez **Allow Any Connection** (Autoriser toute connexion) ou **Only Allow Specific Connections** (Autoriser uniquement des connexions spécifiques).

Si vous choisissez **Only Allow Specific Connections** (Autoriser uniquement des connexions spécifiques), définissez les connexions spécifiques en tant qu'adresses IP, plages d'adresses IP ou plages d'adresse CIDR. Outre l'adresse IP du client, l'adresse IP de l'appliance est automatiquement ajoutée dans la section **User Access** (Accès de l'utilisateur).

Étape 5 Envoyez et validez vos modifications.

Réinitialisation de la phrase secrète de l'administrateur

Before you begin

- Si vous ne connaissez pas la phrase secrète du compte administrateur, communiquez avec votre agent d'assistance client pour réinitialiser la phrase secrète.
- Sachez que les modifications de la phrase secrète prennent effet immédiatement et vous n'êtes pas tenu de les valider.

Tout utilisateur de niveau administrateur peut modifier la phrase secrète de l'utilisateur « admin ».

Étape 1 Sélectionnez **Management Appliance** > **System Administration** > **Users** (Appliance de gestion > Administration système > Utilisateurs).

Étape 2 Cliquez sur le lien **admin** dans la liste Users (Utilisateurs).

Étape 3 Sélectionnez **Change the passphrase** (Modifier la phrase secrète).

Étape 4 Générez ou saisissez la nouvelle phrase secrète.

Configuration de l'adresse de retour pour les messages générés

Vous pouvez configurer l'adresse de retour des courriels générés par AsyncOS pour les rapports.

Étape 1 Choisissez **System Administration > Return Addresses** (Administration système > Adresses de retour).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Saisissez le nom d'affichage, le nom d'utilisateur et le nom de domaine.

Étape 4 Envoyez et validez vos modifications.

Gestion des alertes

Les alertes sont des notifications par courriel contenant des renseignements sur les événements se produisant sur Secure Web Appliance. Ces événements peuvent être de différents niveaux d'importance (ou de gravité), de mineur (informatif) à majeur (critique) et concernent généralement un composant ou une fonctionnalité spécifique de l'appliance.

Note Pour recevoir des alertes et des notifications par courriel, vous devez configurer l'hôte de relais SMTP que l'appliance utilise pour envoyer les courriels.

Classifications et gravités des alertes

Les informations contenues dans une alerte sont déterminées par une classification d'alerte et un niveau de gravité. Vous pouvez préciser quelles classifications d'alertes et quel niveau de gravité sont envoyés à n'importe quel destinataire d'alerte.

Classifications des alertes

AsyncOS envoie les types d'alertes suivants :

- System (Système)
- Matériel
- Programme de mise à jour
- Proxy Web
- Protection contre les programmes malveillants
- AMP
- L4 Traffic Monitor (Supervision du trafic de la couche 4)
- Catégories d'URL externes
- Expiration de la politique

Alert Severities (Gravités des alertes)

Des alertes peuvent être envoyées pour les gravités suivantes :

- **Critical** (Critique) : nécessite une attention immédiate.
- **Warning** (Avertissement) : problème ou erreur nécessitant une supervision supplémentaire et une attention potentiellement immédiate.
- **Information** : informations générées dans le cadre du fonctionnement de routine de cet appareil.

Gestion des destinataires des alertes

Note Si vous avez activé AutoSupport (AutoAssistance) lors de la configuration du système, l'adresse de messagerie que vous avez spécifiée recevra des alertes pour toutes les gravités et toutes les classes par défaut. Vous pouvez modifier cette configuration à tout moment.

Ajout et modification de destinataires d'alertes

Étape 1 Choisissez **System Administration > Alerts** (Administration système > Alertes).

Étape 2 Cliquez sur un destinataire dans la liste des destinataires des alertes pour le modifier ou cliquez sur **Add Recipient** (Ajouter un destinataire) pour ajouter un nouveau destinataire.

Étape 3 Ajoutez ou modifiez l'adresse de messagerie du destinataire. Il est possible d'entrer des adresses multiples, séparées par des virgules.

Étape 4 Sélectionnez les gravités d'alerte à recevoir pour chaque type d'alerte.

Étape 5 Envoyez et validez vos modifications.

Suppression de destinataires d'alertes

Étape 1 Choisissez **System Administration > Alerts** (Administration système > Alertes).

Étape 2 Cliquez sur l'icône de la corbeille correspondant au destinataire de l'alerte dans la liste des destinataires des alertes, puis confirmez.

Étape 3 Validez vos modifications.

Configuration des paramètres d'alerte

Les paramètres d'alertes sont des paramètres globaux, ce qui signifie qu'ils affectent le comportement de toutes les alertes.

Étape 1 Choisissez **System Administration > Alerts** (Administration système > Alertes).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Configurez les paramètres d'alerte selon les besoins.

Option	Description
Adresse de l'expéditeur à utiliser lors de l'envoi d'alertes	L'adresse « Header from: » conforme à RFC 2822 à utiliser pour l'envoi d'alertes. Une option est fournie pour générer automatiquement une adresse en fonction du nom d'hôte du système (« alert@<hostname> »)

Option	Description
Attendez avant d'envoyer une alerte en double	Indique l'intervalle de temps pour les alertes en double. Il existe deux paramètres : **Initial Number of Seconds to Wait Before Sending a Duplicate Alert** (Nombre initial de secondes à attendre avant d'envoyer une alerte en double). Si vous réglez cette valeur sur 0, les résumés d'alertes en double ne sont pas envoyés mais toutes les alertes en double sont envoyées sans délai (une grande quantité de courriels peut être générée sur une courte période). Le nombre de secondes à attendre entre l'envoi d'alertes en double (intervalle d'alerte) augmente après l'envoi de chaque alerte. L'augmentation correspond au nombre de secondes d'attente plus deux fois le dernier intervalle. Ainsi, une attente de 5 secondes verrait les alertes envoyées à 5 secondes, 15, secondes, 35 secondes, 75 secondes, 155 secondes, 315 secondes, etc. **Maximum Number of Seconds to Wait Before Sending a Duplicate Alert** (Nombre maximal de secondes à attendre avant d'envoyer une alerte en double). Vous pouvez définir un nombre maximal de secondes d'attente entre les intervalles de la valeur du nombre maximal de secondes à attendre avant d'envoyer un champ d'alerte en double. Par exemple, si vous définissez la valeur initiale à 5 secondes et la valeur maximale à 60 secondes, des alertes seront envoyées après 5 secondes, 15 secondes, 35 secondes, 60 secondes, 120 secondes, etc.

Note À partir d'AsyncOS 12.0, l'option Cisco AutoSupport est supprimée des paramètres d'alerte. Vous pouvez uniquement activer ou désactiver la fonctionnalité AutoSupport en utilisant l'interface de ligne de commande **alertconfig**.

Étape 4 Envoyez et validez vos modifications.

Listes des alertes

Les sections suivantes répertorient les alertes par classification. Le tableau dans chaque section comprend le nom de l'alerte (descripteur utilisé en interne), le texte de l'alerte, la description, la gravité (critique, information ou avertissement) et les paramètres (le cas échéant) inclus dans le texte du message.

Alertes matérielles

Le tableau suivant contient une liste des différentes alertes matérielles qui peuvent être générées par AsyncOS, y compris une description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
Un événement RAID est survenu : $error	Avertissement	**$error :** le texte de l'erreur RAID.

Alertes système

Le tableau suivant contient une liste des différentes alertes du système qui peuvent être générées par AsyncOS, y compris une description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
Script de démarrage $name sorti avec l'erreur : $message	Critique.	**$name :** nom du script. **$message :** texte du message d'erreur.
Échec de l'arrêt du système : $exit_status : $output',	Critique.	**$exit_status :** code de sortie de la commande. **$output :** sortie de la commande.
Échec du redémarrage du système : $exit_status : $output	Critique.	**$exit_status :** code de sortie de la commande. **$output :** sortie de la commande.
Le processus $name a répertorié la $dependency comme dépendance, mais elle n'existe pas.	Critique.	**$name :** nom du processus. **$dependency :** nom de la dépendance répertoriée.
Le processus $name a répertorié la $dependency comme une dépendance, mais la $dependency n'est pas un processus allow_init.	Critique.	**$name :** nom du processus. **$dependency :** nom de la dépendance répertoriée.
Le processus $name s'est répertorié comme une dépendance.	Critique.	**$name :** nom du processus.
Le processus $name a répertorié la $dependency comme dépendance à plusieurs reprises.	Critique.	**$name :** nom du processus. **$dependency :** nom de la dépendance répertoriée.
Cycle de dépendance détecté : $cycle.	Critique.	**$cycle :** la liste des noms de processus impliqués dans le cycle.
Une erreur s'est produite lors de la tentative de partage de données statistiques à l'aide de la fonctionnalité de participation au réseau. Veuillez transmettre ces informations de suivi à votre fournisseur d'assistance : Erreur : $error.	Avertissement.	**$error :** message d'erreur associé à l'exception.
Il y a une erreur avec « $name ».	Critique.	**$name :** nom du processus qui a généré un fichier principal.
Une erreur d'application est survenue : « $error »	Critique.	**$error :** le texte de l'erreur, généralement un retour en arrière.

Message	Gravité de l'alerte	Paramètres
Appliance : $appliance, Utilisateur : $username, IP source : $ip, Événement : compte verrouillé en raison de X tentatives de connexion infructueuses. L'utilisateur $username a été verrouillé après X échecs de connexion consécutifs. La dernière tentative de connexion datait de $ip.	de l'autre partie.	**$appliance** : identifiant de l' Secure Web Appliance spécifique. **$username** : Identifiant du compte d'utilisateur spécifique. **$ip** : l'adresse IP à partir de laquelle la tentative de connexion a eu lieu.
Assistance technique : le tunnel de service a été activé, le port $port	de l'autre partie.	**$port :** numéro de port utilisé pour le tunnel de service.
Assistance technique : le tunnel de service a été désactivé.	de l'autre partie.	Sans objet.
• L'hôte $ip a été ajouté à la liste des personnes bloquées en raison d'une attaque SSH DOS. • L'hôte de $ip a été ajouté de façon permanente à la liste des autorisations SSH. • L'hôte à l'adresse $ip a été supprimé de la liste des hôtes bloqués.	Avertissement.	**$ip** : adresse IP à partir de laquelle une tentative de connexion a eu lieu. **Description :** Les adresses IP qui tentent de se connecter à l'appliance par SSH, mais qui ne fournissent pas d'informations d'authentification valides, sont ajoutées à la liste des utilisateurs bloqués SSH si plus de 10 tentatives se soldent par un échec en l'espace de deux minutes. Lorsqu'un utilisateur se connecte avec succès à partir de la même adresse IP, cette adresse IP est ajoutée à la liste des personnes autorisées. Les adresses figurant dans la liste des adresses autorisée sont autorisées à accéder même si elles figurent aussi dans la liste des adresses bloquées. Les entrées sont automatiquement supprimées de la liste des personnes bloquées après environ une journée.

Note Les alertes du système comprennent les alertes de clés de fonctionnalité, les alertes de journalisation et les alertes de rapports. Vous recevrez ces alertes après les avoir configurées dans les alertes du système.

Alertes liées aux clés de fonctionnalité

Le tableau suivant contient une liste des différentes alertes de clés de fonctionnalité qui peuvent être générées par AsyncOS, notamment la description de l'alerte et sa gravité :

Message	Gravité de l'alerte	Paramètres
Une clé « $feature » a été téléchargée à partir du serveur de clés et placée dans la zone en attente. Acceptation du CLUF requise.	de l'autre partie.	**$feature :** nom de la fonctionnalité.
Votre clé d'évaluation « $feature » a expiré. Veuillez communiquer avec votre représentant Cisco autorisé.	Avertissement.	**$feature :** nom de la fonctionnalité.
Votre clé d'évaluation « $feature » expirera dans moins de $days jour(s). Veuillez communiquer avec votre représentant Cisco autorisé.	Avertissement.	**$feature :** nom de la fonctionnalité. **$days :** le nombre de jours qui s'écoulent avant l'expiration de la clé de fonctionnalité.

Journalisation des alertes

Le tableau suivant contient une liste des différentes alertes de journalisation qui peuvent être générées par AsyncOS, notamment une description de l'alerte et sa gravité :

Message	Gravité de l'alerte	Paramètres
$error.	de l'autre partie.	**$error :** chaîne de recherche de la source de l'erreur.
Erreur de journal : Abonnement $name : La partition du journal est pleine.	Critique.	**$name :** Nom de l'abonnement au journal.
Erreur de journal : Erreur de transmission pour l'abonnement $name : La connexion à $ip a échoué : $reason.	Critique.	**$name :** Nom de l'abonnement au journal. **$ip :** Adresse IP de l'hôte distant. **$reason :** Texte décrivant l'erreur de connexion
Erreur de journal : Erreur de transmission pour l'abonnement $name : Une commande FTP a échoué sur $ip : $reason.	Critique.	**$name :** Nom de l'abonnement au journal. **$ip :** Adresse IP de l'hôte distant. **$reason :** Texte décrivant ce qui n'a pas fonctionné.

Message	Gravité de l'alerte	Paramètres
Erreur de journal : Erreur de transmission pour l'abonnement $name : SCP n'a pas pu être transféré vers $ip:$port : $reason.	Critique.	**$name :** Nom de l'abonnement au journal. **$ip :** Adresse IP de l'hôte distant. **$port :** Numéro de port sur l'hôte distant. **$reason :** Texte décrivant ce qui n'a pas fonctionné.
Erreur de journal : Abonnement $name : Échec de la connexion à $hostname ($ip) : $error.	Critique.	**$name :** Nom de l'abonnement au journal. **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog. **$error :** Texte du message d'erreur.
Erreur de journal : Abonnement $name : Erreur de réseau lors de l'envoi des données du journal au serveur syslog $hostname ($ip) : $error	Critique.	**$name :** Nom de l'abonnement au journal. **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog. **$error :** Texte du message d'erreur.
Abonnement $name : Expiré $timeout secondes après l'envoi de données au serveur syslog $hostname ($ip).	Critique.	**$name :** Nom de l'abonnement au journal. **$timeout :** Délai d'expiration (en secondes) **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog.
Abonnement $name : Le serveur Syslog $hostname ($ip) n'accepte pas les données assez rapidement.	Critique.	**$name :** Nom de l'abonnement au journal. **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog.

Message	Gravité de l'alerte	Paramètres
Abonnement $name : Le ou les fichiers de journaux les plus anciens ont été supprimés, car les fichiers journaux ont atteint le nombre maximal de $max_num_files. Les fichiers supprimés sont les suivants : $files_removed.	de l'autre partie.	**$name :** Nom de l'abonnement au journal. **$max_num_files :** Nombre maximal de fichiers autorisés par abonnement au journal. **$files_removed :** Liste des fichiers qui ont été supprimés.

Rapport d'alertes

Le tableau suivant contient la liste des différentes alertes de rapport qui peuvent être générées par AsyncOS, notamment une description de l'alerte et de la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
Le système de rapports n'est pas en mesure de maintenir le débit des données générées. Toutes les nouvelles données générées seront perdues.	Critique.	Sans objet.
Le système de rapports est maintenant en mesure de gérer de nouvelles données.	de l'autre partie.	Sans objet.
Un échec s'est produit lors de la création du rapport périodique « $report_title ». Cet abonnement doit être examiné et supprimé si ses détails de configuration ne sont plus valides.	Critique.	**$report_title :** titre du rapport.
Un échec est survenu lors de l'envoi par courriel du rapport périodique « $report_title ». Cet abonnement a été supprimé du planificateur.	Critique.	**$report_title :** titre du rapport.
Le traitement des données de rapport recueillies a été désactivé en raison d'un manque d'espace disque de journalisation. L'utilisation du disque est supérieure au pourcentage du seuil $threshold. L'enregistrement des événements de rapport sera bientôt limité, et des données de rapport pourraient être perdues si de l'espace disque n'est pas libéré (en supprimant les anciens journaux, etc.). Une fois que l'utilisation du disque passe sous le pourcentage du seuil $threshold, le traitement complet des données de rapport sera redémarré automatiquement.	Avertissement.	**$threshold** : valeur de seuil.

Message	Gravité de l'alerte	Paramètres
RAPPORTS PÉRIODIQUES : lors de la création du rapport périodique « $report_title », le fichier de spécification de domaine attendu est introuvable dans « $file_name ». Aucun rapport n'a été envoyé.	Critique.	**$report_title :** titre du rapport. **$file_name** : nom du fichier.
Le groupe de compteurs « $counter_group » n'existe pas.	Critique.	**$counter_group** : nom de counter_group.
RAPPORTS PÉRIODIQUES : lors de la création du rapport périodique « $report_title », le fichier de spécification de domaine « $file_name » était vide. Aucun rapport n'a été envoyé.	Critique.	**$report_title :** titre du rapport. **$file_name** : nom du fichier.
RAPPORTS PÉRIODIQUES : des erreurs ont été rencontrées lors du traitement du fichier de spécification de domaine « $file_name » pour le rapport périodique « $report_title ». Toute ligne sur laquelle un problème a été signalé n'a fait l'objet d'aucun rapport envoyé. $error_text	Critique.	**$report_title :** titre du rapport. **$file_name** : nom du fichier. **$error_text** : liste des erreurs rencontrées.
Le traitement des données de rapport recueillies a été désactivé en raison d'un manque d'espace disque de journalisation. L'utilisation du disque est supérieure au pourcentage du seuil $threshold. L'enregistrement des événements de rapport sera bientôt limité, et des données de rapport pourraient être perdues si de l'espace disque n'est pas libéré (en supprimant les anciens journaux, etc.). Une fois que l'utilisation du disque passe sous le pourcentage du seuil $threshold, le traitement complet des données de rapport sera redémarré automatiquement.	Avertissement.	**$threshold** : valeur de seuil.
Le système de rapports a rencontré une erreur critique lors de l'ouverture de la base de données. Afin d'éviter d'interrompre d'autres services, les rapports ont été désactivés sur cette appliance. Veuillez contacter l'assistance client pour activer la création de rapports. Le message d'erreur est le suivant : $err_msg	Critique.	**$err_msg** : texte du message d'erreur.

Alertes du programme de mise à jour

Le tableau suivant contient une liste des différentes alertes du programme de mise à jour qui peuvent être générées par AsyncOS, notamment la description de l'alerte et la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
L'application $app a essayé et échoué $attempts fois de terminer une mise à jour avec succès. Cela peut être dû à un problème de configuration réseau ou à une panne temporaire.	Avertissement.	**$app :** Secure Web Appliance nom du service de sécurité. **$attempts :** nombre de tentatives.
Le programme de mise à jour n'a pas pu communiquer avec le serveur de mise à jour depuis au moins $threshold.	Avertissement.	**$threshold :** durée de la valeur de seuil.
Erreur inconnue survenue : $traceback.	Critique.	**$traceback :** informations de recherche de la source.
Révoquer de certificat : échec de validation OCSP du certificat de serveur de mise à jour ($host:$port). Assurez-vous que le certificat est valide.	Éléments essentiels	**$host:** nom d'hôte du serveur de mise à jour. **$port :** port du serveur de mise à jour.

Alertes de protection contre les programmes malveillants

Pour plus d'informations sur les alertes relatives à Cisco Secure Endpoint, consultez Veiller à recevoir des alertes sur les problèmes Cisco Secure Endpoint , on page 339.

Alertes AMP

Le tableau suivant contient une liste des différentes alertes AMP qui peuvent être générées par AsyncOS, y compris la description des alertes et leur gravité :

Message	Gravité de l'alerte	Paramètres
Échec de l'enregistrement de l'appliance auprès de la console AMP for Endpoints. $error	Avertissement	**$error :**message d'erreur.
Échec du désenregistrement de l'appliance ($devname) de la console AMP for Endpoints $error	Avertissement	**$devname:**nom du périphérique. **$error :**message d'erreur.

Alertes du proxy Web

Le tableau suivant contient la liste des différentes alertes de proxy Web qui peuvent être générées par AsyncOS, y compris la description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
Une erreur s'est produite lors de l'opération de lecture/écriture sur le disque. $error	Information	**$info :**informations supplémentaires telles que l'objet et la taille de l'objet en cours d'écriture.
Le proxy Web a détecté que le contenu de la partition de mise en cache n'est pas valide. La purge du cache pourrait résoudre le problème : $errorstring	Information	**$errorstring :** informations supplémentaires sur le motif de l'invalidité du contenu du cache.
Erreurs des paramètres de configuration. $errorstring	Avertissement	**$errorstring :** description détaillée des erreurs de valeur de paramètre, notamment du paramètre et de sa valeur.
Le total des connexions côté client a dépassé le seuil défini. Les connexions persistantes sont temporairement désactivées. $info	Avertissement	**$info :** informations supplémentaires.
Le routeur WCCPv2 configuré ne répond pas ou est inaccessible. $info	Avertissement	**$info :** informations supplémentaires.
Le proxy de transmission en amont configuré ne répond pas ou est inaccessible. $info	Avertissement	**$info :** informations supplémentaires.
Le processus du proxy Web n'a pas de mémoire et a redémarré. $info	Avertissement	**$info :** informations supplémentaires.
Une erreur s'est produite dans la bibliothèque snmp. $info	Avertissement	**$info :** informations supplémentaires telles que la demande snmp en question.
Diverses erreurs ont entraîné la fermeture du proxy Web. $info	Avertissement	**$info :** informations supplémentaires, le cas échéant.
Le processus DNS s'est arrêté. $info	Avertissement	**$info :** informations supplémentaires, le cas échéant.
Le processus d'authentification s'est arrêté. $info	Avertissement	**$info :** informations supplémentaires, le cas échéant.

Message	Gravité de l'alerte	Paramètres
Le proxy Web n'a pas pu réserver de mémoire pour les principales structures de données internes lors du démarrage du processus. $info	Éléments essentiels	**$info :**informations supplémentaires telles que la taille de diverses structures de données internes principales.
Une erreur s'est produite lors de l'opération de lecture/écriture sur le disque. $info	Éléments essentiels	**$info :**informations supplémentaires telles que l'objet et la taille de l'objet en cours d'écriture.

Alertes de catégories d'URL externes

Le tableau suivant contient une liste des diverses alertes de catégories d'URL externes qui peuvent être générées par AsyncOS, notamment une description de l'alerte et la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
$errmsg	Avertissement	**$errmsg** : message d'erreur.
$errmsg	Information	**$errmsg** : message d'erreur.
$errmsg	Éléments essentiels	**$errmsg** : message d'erreur.

L4 Traffic Monitor Alerts (Alertes de la supervision du trafic de la couche 4)

Le tableau suivant contient une liste des différentes alertes de la supervision du trafic de la couche 4 qui peuvent être générées par AsyncOS, notamment une description de l'alerte et de la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
$errmsg	Avertissement	**$errmsg** : message d'erreur.
$errmsg	Information	**$errmsg** : message d'erreur.
$errmsg	Éléments essentiels	**$errmsg** : message d'erreur.

Alertes d'expiration des politiques

Le tableau suivant contient une liste des diverses alertes d'expiration de politique qui peuvent être générées par AsyncOS, y compris une description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
« $PolicyType » : « $GroupName » a été désactivé en raison d'une configuration d'expiration.	Information	**$PolicyType :** politique d'accès/politique de déchiffrement en fonction du type de politique Web. **$GroupName :**nom du groupe de politiques.
'$PolicyType' : '$GroupName' expirera dans jours : 3.	Information	**$PolicyType :** politique d'accès/politique de déchiffrement en fonction du type de politique Web. **$GroupName :**nom du groupe de politiques.

Conformité à la norme FIPS

Les normes Federal Information Processing Standards (FIPS) précisent les exigences relatives aux modules cryptographiques utilisés par tous les organismes gouvernementaux pour protéger les informations sensibles, mais non classifiées. Les normes FIPS aident à assurer la conformité aux exigences fédérales en matière de sécurité et de confidentialité des données. Les normes FIPS, mises au point par le National Institue for Standards and Technology (NIST), sont destinées à être utilisées lorsqu'aucune norme volontaire n'existe pour répondre aux exigences fédérales.

Secure Web Appliance est conforme à la norme FIPS 140-2 en mode FIPS grâce au module cryptographique commun de Cisco (C3M). Le mode FIPS est désactivé par défaut.

Note **À partir de la version AsyncOS 15.0, le mode des normes fédérales de traitement de l'information (FIPS) n'est pas pris en charge.**

Thèmes connexes

- Problèmes du mode FIPS, on page 634

Exigences du certificat FIPS

Le mode FIPS exige que tous les services de chiffrement activés sur le Secure Web Appliance utilisent un certificat conforme aux normes FIPS. Cela s'applique aux services de chiffrement suivants :

- Proxy HTTPS
- Authentification
- Fournisseur d'identité pour SaaS
- Service HTTPS de gestion d'appliances

- Configuration de la DLP externe pour ICAP sécurisé
- Identity Service Engine (ISE)
- Configuration SSL
- Configuration SSH

Note Le service HTTPS de gestion d'appliances doit être configuré avec un certificat de plainte FIPS pour que le mode FIPS puisse être activé. Il n'est pas nécessaire d'activer les autres services de chiffrement.

Un certificat conforme aux normes FIPS doit satisfaire aux exigences suivantes :

Certificate (certificat)	Algorithme	Signature Algorithm (algorithme de signature)	Notes
X509	RSA	sha1WithRSAEncryption sha256WithRSAEncryption	Cisco recommande une clé de 1024 bits pour des performances de déchiffrement optimales et une sécurité suffisante. Une taille en bits plus grande augmentera la sécurité, mais aura une incidence sur les performances de déchiffrement.

FIPS Certificate Validation (Validation du certificat FIPS)

Lorsque vous activez le mode FIPS, l'appliance effectue les vérifications de certificat suivantes :

- Tous les certificats chargés dans Secure Web Appliance, que ce soit au moyen de l'interface utilisateur ou de la commande de l'interface de ligne de commande `certconfig`, sont validés strictement conformes aux normes CC. Aucun certificat sans chemin approuvé approprié dans le magasin des certificats approuvés de Secure Web Appliance ne peut être chargé.
- Signature de certificat avec une validation de chemin approuvé; altération de certificats ou de clés publiques avec ensemble `basicConstrains` et `CAFlag` validé pour tous les certificats du signataire.
- La validation OCSP est disponible pour valider un certificat par rapport à une liste de révocation. Ce paramètre peut être configuré à l'aide de la commande de l'interface de ligne de commande `certconfig`.

Remarque Une nouvelle sous-commande `OCSPVALIDATION_FOR_SERVER_CERT` est ajoutée à la commande `certconfig` de l'interface de ligne de commande principale. La nouvelle sous-commande vous permet d'activer la validation OCSP pour les certificats de serveur LDAP et de mise à jour. Si la validation des certificats est activée, vous recevrez une alerte si les certificats impliqués dans la communication sont révoqués.

Voir aussi Validation stricte du certificat, à la page 608.

Activation ou désactivation du mode FIPS

Before you begin

- Effectuez une copie de sauvegarde de la configuration de l'appliance; voir Enregistrement du fichier de configuration de l'appliance, on page 556
- Assurez-vous que les certificats à utiliser en mode FIPS utilisent des algorithmes de clé publique approuvés par FIPS 140-2 (voir Exigences du certificat FIPS, on page 603).

Note

- La modification du mode FIPS déclenche un redémarrage de l'appliance.
- Lorsque vous désactivez le mode FIPS, les paramètres SSL et SSH, qui sont automatiquement devenus conformes aux normes FIPS lorsque le mode FIPS a été activé, ne sont pas réinitialisés à leurs valeurs par défaut. Vous devez explicitement modifier ces paramètres si vous souhaitez permettre à un client utilisant des paramètres SSH/SSL plus faibles de se connecter. Voir Configuration SSL , on page 606 pour de plus amples informations.

Étape 1 Choisissez **System Administration > FIPS Mode** (Administration système > Modèle FIPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez la case **Enable FIPS Compliance** (Activer la conformité FIPS) pour activer la conformité FIPS.

Lorsque vous cochez la case Enable FIPS Compliance (Activer la conformité FIPS), la case **Enable encryption of Critical Senstive Settings (CSP)** (Activer le chiffrement des paramètres critiques sensibles (CSP) est activée.

Étape 4 Cochez la case **Enable encryption of Critical Senstive Settings (CSP)** (Activer le chiffrement des paramètres critiques sensibles (CSP) pour activer le chiffrement des données de configuration comme les mots de passe, les informations d'authentification, les certificats, les clés partagées, etc.

Étape 5 Cliquez sur **Submit** (Soumettre).

Étape 6 Cliquez sur **Continue** (Continuer) pour permettre à l'appliance de redémarrer.

Gestion de la date et de l'heure du système

Définition du fuseau horaire

Étape 1 Choisissez **System Administration > Time Zone** (Administration système > Fuseau horaire).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez votre région, votre pays et votre fuseau horaire ou sélectionnez le décalage GMT.

Étape 4 Envoyez et validez les modifications.

Synchronisation de l'horloge système avec un serveur NTP

Cisco vous recommande de configurer votre Secure Web Appliance pour suivre la date et l'heure actuelles en interrogeant un serveur NTP (Network Time Protocol), et non en réglant manuellement l'heure sur l'appliance. Cela est particulièrement vrai si votre appliance s'intègre à d'autres périphériques. Tous les périphériques intégrés doivent utiliser le même serveur NTP.

Étape 1 Choisissez **System Administration > Time Settings** (Administration système > Paramètres de temps).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Use Network Time Protocol** (Utiliser Network Time Protocol) comme méthode de maintien de l'heure.

Étape 4 Entrez le nom d'hôte complet ou l'adresse IP du serveur NTP, en cliquant sur **Add Row** (Ajouter une ligne) si nécessaire pour ajouter des serveurs.

Étape 5 (Facultatif) Choisissez la table de routage associée à un type d'interface réseau de dispositif, Gestion ou Données, à utiliser pour les requêtes NTP. Il s'agit de l'adresse IP à partir de laquelle les requêtes NTP doivent provenir.

Note Cette option n'est modifiable que si l'appliance utilise le routage fractionné pour le trafic de données et de gestion.

Étape 6 Envoyez et validez vos modifications.

Configuration SSL

Pour une sécurité améliorée, vous pouvez activer et désactiver SSL v3 et diverses versions de TLS pour plusieurs services. Pour une sécurité optimale, il est recommandé de désactiver SSL v3 pour tous les services. Par défaut, toutes les versions de TLS sont activées et SSL est désactivé.

Note Vous pouvez également utiliser la commande de l'interface de ligne de commande `sslconfig` pour activer ou désactiver ces fonctionnalités. Consultez Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671.

Note Redémarrez l'application lorsque vous modifiez la configuration SSL et que cela entraîne la désactivation des chiffrements TLS.

Étape 1 Choisissez **System Administration > SSL Configuration** (Administration système > Configuration SSL).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez les cases correspondantes pour activer SSL v3 et TLS v1.x pour ces services :

- **Appliance Management Web User Interface** (Interface utilisateur Web de gestion d'appliance) : la modification de ce paramètre déconnectera toutes les connexions utilisateur actives.
- **Services de proxy** : inclut le proxy HTTPS et le chiffrement des informations d'authentification pour Secure Client. Cette section comprend également :
  - **Chiffrement à utiliser** : vous pouvez saisir des suites de chiffrement supplémentaires à utiliser avec les communications des services proxy. Utilisez les deux-points (:) pour séparer les suites. Pour empêcher l'utilisation d'un chiffrement particulier, ajoutez un point d'exclamation (!) devant cette chaîne. Par exemple, `!EXP-DHE-RSA-DES-CBC-SHA .`

    Assurez-vous de saisir uniquement des suites appropriées pour les versions TLS/SSL que vous avez vérifiées. Reportez-vous à https://www.openssl.org/docs/manmaster/man1/ciphers.html pour plus d'informations et pour en savoir plus sur les listes de chiffrement.

    L'appliance prend en charge la version TLSv1.3. Le chiffrement `TLS_AES_256_GCM_SHA384` est ajouté à la liste de chiffrement par défaut. Par défaut, TLSv1.3 est activé sur l'appliance.

    Dans AsyncOS version 14.0, les chiffrements `TLS_AES_128_GCM_SHA256` et `TLS_CHACHA20_POLY1305_SHA256` sont ajoutés à la liste de chiffrements par défaut.

    Le chiffrement par défaut pour AsyncOS versions 9.0 et antérieures est `Default:+kEDH`.

    Le chiffrement par défaut pour les versions 9.1 à 11.8 d'AsyncOS est le suivant :

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
    !AES256-SHA:DHE-RSA-AES128-SHA
    ```

    Dans ce cas, le chiffrement par défaut peut changer en fonction de vos sélections de chiffrement ECDHE.

    Le chiffrement par défaut pour AsyncOS versions 12.0 et ultérieures est :

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384
    ```

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
    ```

    Note Mettez à jour la suite de chiffrement par défaut lors de la mise à niveau vers une version plus récente d'AsyncOS. Les suites de chiffrements ne sont pas automatiquement mises à jour. Lorsque vous effectuez une mise à niveau d'une version antérieure vers AsyncOS 12.0 ou une version ultérieure, Cisco recommande de mettre à jour la suite de chiffrement pour :

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384
    ```

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
    ```

  - **Désactiver la compression TLS (recommandé)** – Vous pouvez cocher cette case pour désactiver la compression TLS. Cela est recommandé pour une sécurité optimale.
- **Services LDAP sécurisés** : incluent l'authentification, l'authentification extérieure et Secure Mobility.
- **Services ICAP sécurisés (DLP externe)** : sélectionnez le ou les protocoles utilisés pour sécuriser les communications ICAP entre l'appliance et les serveurs DLP (Data Loss Prevention) externes. Consultez Configuration des serveurs DLP externes, on page 366 pour obtenir de plus amples renseignements.

- **Service de mise à jour** : sélectionnez le ou les protocoles utilisés pour les communications entre l'appliance et les serveurs de mise à jour disponibles. Consultez Mises à niveau et mises à jour d'AsyncOS pour le Web, on page 613 pour en savoir plus sur les services de mise à jour.

Note Les serveurs de mise à jour de Cisco ne prennent pas en charge SSL v3, par conséquent, TLS 1.0 ou une version ultérieure doit être activé pour le service de mise à jour de Cisco. Cependant, SSL v3 peut toujours être utilisé avec un serveur de mise à jour local, s'il est configuré ainsi, vous devez déterminer quelles versions de SSL/TLS sont prises en charge sur ce serveur.

Étape 4 Cliquez sur **Submit** (Soumettre).

Certificate Management

L'appliance utilise des certificats numériques pour établir, confirmer et sécuriser diverses connexions. La page Certificate Management (Gestion des certificats) vous permet d'afficher et de mettre à jour les listes de certificats actuelles, de gérer les certificats racine approuvés et d'afficher les certificats bloqués.

Note La page Certificate Management (Gestion des certificats) prend du temps à se charger et entraîne une erreur d'expiration de délai lorsque l'appliance n'est pas connectée à Internet. En outre, l'erreur de réseau « Failed to fetch manifest » (Échec de la récupération du manifeste) s'affiche dans la liste des mises à jour de certificat après le chargement du certificat.

Thèmes connexes

- À propos des certificats et des clés, on page 609
- Mises à jour des certificats, on page 610
- Gestion des certificats racine approuvés, on page 609
- Affichage des certificats bloqués, on page 610

Validation stricte du certificat

Avec la sortie des mises à jour du mode FIPS dans AsyncOS 10.5, tous les certificats présentés sont validés strictement pour se conformer aux normes Common Criteria (CC) avant le téléchargement, et la validation OCSP est disponible pour valider les certificats par rapport à une liste de révocation.

Vous devez vous assurer que des certificats valides appropriés sont chargés dans Secure Web Appliance et que des certificats sécurisés valides sont configurés sur tous les serveurs associés pour faciliter des liaisons SSL sans interruption avec ces serveurs.

Une validation de certificat stricte est appliquée pour les chargements de certificat suivants :

- Proxy HTTPS [Security Services > HTTPS Proxy (Services de sécurité > Proxy HTTPS)]
- Serveur d'analyse des fichiers [Security Services > Anti-Malware and Reputation > Advanced Settings for File Analysis > File Analysis Server: Private Cloud & Certificate Authority: Use Uploaded Certificate Authority (Services de sécurité > Protection contre les programmes malveillants et réputation > Paramètres avancés pour l'analyse des fichiers > Serveur d'analyse des fichiers : Cloud privé et Autorité de certification)]

- Certificats racine approuvés [Network > Certificate Management (Réseau > Gestion des certificats)]
- Paramètres d'authentification globaux [Network > Authentication > Global Authentication Settings (Réseau > Authentification > Paramètres d'authentification globaux)]
- Fournisseur d'identité pour SaaS [Network > Identity Provider for SaaS (Réseau > Fournisseur d'identité pour SaaS)]
- Moteur du service d'identité [Network > Identity Services Engine (Réseau > Moteur du service d'identité)]
- Serveurs DLP externes [Network > External DLP Servers (Réseau > Serveurs DLP externes)]
- LDAP et LDAP sécurisé [Network > Authentication > Realm (Réseau > Authentification > Domaine)]

Voir aussi Conformité à la norme FIPS, à la page 603.

À propos des certificats et des clés

Lorsqu'un navigateur invite son utilisateur à s'authentifier, le navigateur envoie les informations d'authentification au proxy Web à l'aide d'une connexion sécurisée HTTPS. Par défaut, le Secure Web Appliance utilise le « certificat de démonstration de l'appliance Cisco pour la sécurité du Web » fourni avec pour créer une connexion HTTPS avec le client. La plupart des navigateurs avertissent les utilisateurs que le certificat n'est pas valide. Pour empêcher les utilisateurs de voir le message de certificat non valide, vous pouvez télécharger un certificat et une paire de clés que vos applications reconnaissent automatiquement.

Thèmes connexes

- Chargement ou génération d'un certificat et d'une clé, on page 610
- Requêtes de signature de certificat, on page 611
- Certificats intermédiaires, on page 612

Gestion des certificats racine approuvés

Le Secure Web Appliance est livré avec et gère une liste de certificats racine approuvés. Les sites Web dotés de certificats approuvés n'ont pas besoin de déchiffrement.

Vous pouvez gérer la liste des certificats approuvés, en y ajoutant et en en supprimant fonctionnellement des certificats. Bien que Secure Web Appliance ne supprime pas les certificats de la liste principale, il vous permet de remplacer la confiance dans un certificat, ce qui supprime fonctionnellement le certificat de la liste approuvée.

Pour ajouter, remplacer ou télécharger un certificat racine approuvé :

Étape 1 Choisissez **Network** > **Certificate Management** (Réseau > Gestion des certificats).

Étape 2 Cliquez sur **Manage Trusted root Certificates** (Gestion des certificats racine approuvés) sur la page Certificate Management (Gestion des certificats).

Étape 3 Pour ajouter un certificat racine approuvé personnalisé avec une autorité de signature ne figurant pas dans la liste des autorités reconnues par Cisco :

Cliquez sur **Import** (Importer), puis recherchez, sélectionnez et **envoyez** le fichier de certificat.

Étape 4 Pour remplacer la fiabilité d'un ou de plusieurs certificats reconnus par Cisco :

a) Cochez la case **Override Trust** (Remplacer la fiabilité) pour chaque entrée que vous souhaitez remplacer.
b) Cliquez sur **Submit** (Soumettre).

Étape 5 Pour télécharger une copie d'un certificat en particulier :

a) Cliquez sur le nom du certificat dans la liste des certificats racine approuvés de Cisco pour développer cette entrée.
b) Cliquez sur **Download Certificate** (Télécharger le certificat).

Mises à jour des certificats

La section Updates (Mises à jour) répertorie la version et les dernières informations mises à jour pour les ensembles de certificats racine approuvés et de listes bloquées de Cisco sur l'appliance. Ces ensembles sont régulièrement mis à jour.

Cliquez sur **Update Now** (Mettre à jour maintenant) dans la page Certificate Management (Gestion des certificats) pour mettre à jour tous les ensembles pour lesquels des mises à jour sont disponibles.

Affichage des certificats bloqués

Pour afficher une liste des certificats que Cisco a déterminés comme non valides et qu'il a bloqués :

Cliquez sur **View Blocked Certificates** (Afficher les certificats bloqués).

Chargement ou génération d'un certificat et d'une clé

Certaines fonctionnalités d'AsyncOS nécessitent un certificat et une clé pour établir, confirmer ou sécuriser une connexion, le moteur de services d'identité et. Vous pouvez soit charger un certificat et une clé existants, soit en générer un lorsque vous configurez la fonctionnalité.

Chargement d'un certificat et d'une clé

Un certificat que vous chargez sur l'appliance doit satisfaire aux exigences suivantes :

- Il doit utiliser la norme X.509.
- Il doit inclure une clé privée correspondante au format PEM. Format DER non pris en charge.

Étape 1 Sélectionnez **Use Uploaded Certificate and Key** (Utiliser le certificat et la clé téléchargés).

Étape 2 Dans le champ **Certificate** (Certificat), cliquez sur Browse (Parcourir); localisez le fichier à télécharger.

Note Le proxy Web utilise le premier certificat ou la première clé du fichier. Le fichier de certificat doit être au format PEM. Format DER non pris en charge.

Étape 3 Dans le champ **Key** (Clé), cliquez sur Browse (Parcourir); localisez le fichier à télécharger.

Note La longueur de la clé doit être de 512, 1024 ou 2048 bits. Le fichier de clé privée doit être au format PEM. Format DER non pris en charge.

Étape 4 Si la clé est chiffrée, sélectionnez **Key is Encrypted** (La clé est chiffrée).

Étape 5 Cliquez sur **Upload Files** (Charger des fichiers).

Génération d'un certificat et d'une clé

Étape 1 Sélectionnez **Use Generate Certificate and Key** (Utiliser le certificat et la clé générés).

Étape 2 Cliquez sur **Generate New Certificate and Key** (Générer un nouveau certificat et une nouvelle clé).

a) Dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé), saisissez les renseignements nécessaires à la génération.

Note Vous pouvez saisir n'importe quel caractère ASCII, à l'exception de la barre oblique (/) dans le champ Common Name (Nom commun).

b) Cliquez sur **Generate** (Générer) dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé).

Une fois la génération terminée, les informations sur le certificat s'affichent dans la section Certificate (Certificat) ainsi que deux liens : **Download Certificate** (Télécharger le certificat) et **Download Certificate Signing Request** (Télécharger la demande de signature de certificat). En outre, il existe une option de certificat signé qui est utilisée pour télécharger le certificat signé lorsque vous le recevez de l'autorité de certification (CA).

Étape 3 Cliquez sur **Download Certificate** (Télécharger le certificat) pour télécharger le nouveau certificat et le charger sur l'appliance.

Étape 4 Cliquez sur **Download Certificate Signing Request** (Télécharger la demande de signature de certificat) pour télécharger le nouveau fichier de certificat et le transmettre à une autorité de certification (AC) pour signature. Consultez Requêtes de signature de certificat, on page 611 pour en savoir plus sur ce processus.

a) Lorsque l'autorité de certification renvoie le certificat signé, cliquez sur Browse (Parcourir) dans la partie Signed Certificate (Certificat signé) du champ Certificate (Certificat) pour identifier le fichier de certificat signé, puis cliquez sur Upload File (Charger le fichier) pour le charger sur l'appliance.

b) Assurez-vous que le certificat racine de l'autorité de certification est présent dans la liste des certificats racine approuvés de l'appliance. Si ce n'est pas le cas, ajoutez-le. Consultez la Gestion des certificats racine approuvés, on page 609 pour de plus amples renseignements.

Requêtes de signature de certificat

Secure Web Appliance ne peut pas générer de demandes de signature de certificat (CSR) pour les certificats téléchargés sur l'appliance. Par conséquent, pour qu'un certificat soit créé pour l'appliance, vous devez émettre la demande de signature à partir d'un autre système. Enregistrez la clé au format PEM à partir de ce système, car vous devrez l'installer sur l'appliance plus tard.

Vous pouvez utiliser n'importe quel ordinateur UNIX sur lequel une version récente d'OpenSSL est installée. Veillez à indiquer le nom d'hôte de l'appliance dans la demande de signature de certificat (CSR). Suivez les directives à l'emplacement suivant pour obtenir des renseignements sur la génération d'une requête de signature de certificat (CSR) à l'aide d'OpenSSL :

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

Une fois la demande de signature de certificat (CSR) générée, envoyez-la à une autorité de certification (AC). L'autorité de certification renverra le certificat au format PEM.

Si vous obtenez un certificat pour la première fois, recherchez sur Internet « certificats de serveur de services d'autorité de certification SSL » et choisissez le service qui répond le mieux aux besoins de votre entreprise. Suivez les instructions du service pour obtenir un certificat SSL.

Note Vous pouvez également générer et signer votre propre certificat. Les outils nécessaires sont inclus avec OpenSSL, le logiciel gratuit disponible à l'adresse `http://www.openssl.org` .

Certificats intermédiaires

Outre la vérification du certificat de l'autorité de certification racine, AsyncOS prend en charge la vérification des certificats intermédiaires. Les certificats intermédiaires sont des certificats émis par une autorité de certification racine approuvée qui sont ensuite utilisés pour créer des certificats supplémentaires. Cela crée une ligne de confiance en chaîne. Par exemple, un certificat peut être émis par le site exemple.com qui, à son tour, se voit accorder les droits d'émettre des certificats par une autorité de certification racine approuvée. Le certificat émis par le site exemple.com doit être validé par rapport à la clé privée du site exemple.com ainsi que par rapport à la clé privée de l'autorité de certification racine approuvée.

Les serveurs envoient une « chaîne de certificats » dans une liaison SSL pour que les clients (par exemple, les navigateurs et, dans ce cas, le Secure Web Appliance, qui est un proxy HTTPS) authentifient le serveur. Normalement, le certificat du serveur est signé par un certificat intermédiaire qui, à son tour, est signé par un certificat racine approuvé et, pendant la liaison, le certificat du serveur et la chaîne complète de certificats sont présentés au client. Comme le certificat racine est généralement présent dans le magasin de certificats approuvés de Secure Web Appliance, la chaîne de certificats est vérifiée avec succès.

Cependant, il peut parfois arriver, lorsque le certificat de l'entité terminale est modifié sur le serveur, que les mises à jour nécessaires pour la nouvelle chaîne ne soient pas effectuées. Par conséquent, à partir de maintenant, le serveur présente uniquement le certificat de serveur lors de l'établissement de la liaison SSL et le proxy Secure Web Appliance ne peut pas vérifier la chaîne de certificats, car le certificat intermédiaire est manquant.

Auparavant, la solution consistait en l'intervention manuelle de l'administrateur Secure Web Appliance, qui téléchargeait le certificat intermédiaire nécessaire dans le magasin de certificats approuvés. Vous pouvez désormais utiliser la commande d'interface de ligne de commande `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` (advancedproxyconfig > HTTPS > Voulez-vous activer la découverte et le téléchargement automatiques des certificats intermédiaires manquants?) pour activer la « découverte de certificats intermédiaires », un processus que Secure Web Appliance utilise afin d'éliminer l'étape manuelle dans ces situations.

La découverte de certificats intermédiaires utilise une méthode appelée « analyse AIA » : lorsqu'un certificat non fiable se présente, l'appliance Secure Web Appliance l'examine pour détecter une extension nommée « Authority Information Access ». Cette extension comprend un champ facultatif URI pour les émetteurs de l'autorité de certification, qui peuvent être interrogés pour le certificat de l'émetteur utilisé pour signer le certificat du serveur en question. Si le certificat de l'émetteur est disponible, Secure Web Appliance le récupère de manière récursive jusqu'à ce que le certificat de l'autorité de certification racine soit obtenu, puis tente à nouveau de vérifier la chaîne.

Mises à niveau et mises à jour d'AsyncOS pour le Web

Cisco publie régulièrement des mises à niveau (nouvelles versions de logiciels) et des mises à jour (modifications des versions logicielles actuelles) pour AsyncOS pour le Web et ses composants.

Meilleures pratiques pour la mise à niveau d'AsyncOS pour le Web

- Avant de lancer la mise à niveau, enregistrez le fichier de configuration XML à partir de Secure Web Appliance, de la page **System Administration > Configuration File** (Administration système > Fichier de configuration) ou en utilisant la commande saveconfig.
- Enregistrez d'autres fichiers stockés sur l'appliance, tels que les fichiers PAC ou les pages de notification personnalisée à l'utilisateur final.
- Lors de la mise à niveau, ne faites pas de pause pendant de longues périodes aux différentes invites. Si la session TCP expire pendant le téléchargement, la mise à niveau pourrait échouer.
- Une fois la mise à niveau terminée, enregistrez les informations de configuration dans un fichier XML.

Thèmes connexes

- Enregistrement, chargement et réinitialisation de la configuration de l'appliance, on page 556

Mise à niveau et mise à jour d'AsyncOS et des composants du service Security

Téléchargement et installation d'une mise à niveau

Avant de commencer

Enregistrez le fichier de configuration de l'appliance (voir Enregistrement, chargement et réinitialisation de la configuration de l'appliance, à la page 556).

Remarque Lors du téléchargement et de la mise à niveau d'AsyncOS en une seule opération à partir d'un serveur local plutôt que d'un serveur Cisco, la mise à niveau est installée immédiatement lors du téléchargement. Une bannière s'affiche pendant 10 secondes au début du processus de mise à niveau. Pendant que cette bannière est affichée, vous pouvez taper Ctrl-C pour quitter le processus de mise à niveau avant le début du téléchargement.

Remarque Lors d'une mise à niveau, si le certificat d'authentification sécurisée n'est pas conforme aux normes FIP, il sera remplacé par le certificat par défaut du dernier chemin vers lequel votre appliance est mise à niveau. Cela se produit uniquement lorsque le client a utilisé le certificat par défaut avant la mise à niveau.

Vous pouvez télécharger et installer en une seule opération, ou télécharger en arrière-plan et installer plus tard.

La mise à niveau échoue si une valeur de configuration stockée dans les fichiers varstore comporte des caractères non ASCII.

Étape 1 Choisissez **System Administration** > **System Upgrade** (Administration système > Mise à niveau du système).

Étape 2 Cliquez sur **Upgrade Options** (Options de mise à niveau).

Sélectionnez les options de mise à niveau et une image de mise à niveau :

Paramètres	Description
Choisir une option de mise à niveau	• **Download and install** (Télécharger et installer) : téléchargez et installez la mise à niveau en une seule opération. Si vous avez déjà téléchargé un programme d'installation, vous serez invité à remplacer le téléchargement existant. • **Download only** (Télécharger seulement) : téléchargez un programme d'installation de mise à niveau, mais ne l'installez pas. Si vous avez déjà téléchargé un programme d'installation, vous serez invité à remplacer le téléchargement existant. Le programme d'installation se télécharge en arrière-plan sans interrompre le service. Un bouton **Install** (Installer) s'affiche lorsque le téléchargement est terminé; cliquez pour installer une mise à niveau déjà téléchargée.
	Sélectionnez une image de mise à niveau à télécharger, ou à télécharger et installer, dans le champ **List of available upgrade images files at upgrade server** (Liste des fichiers image de mise à niveau disponibles sur le serveur de mise à niveau).
Préparation de la mise à niveau	• Pour enregistrer une copie de sauvegarde de la configuration actuelle dans le répertoire **`configuration`** de l'appliance, cochez l'option **Save the current configuration to the configuration directory before upgrading** (Enregistrer la configuration actuelle dans le répertoire de configuration avant la mise à niveau). • Si l'option **Save current configuration** (Enregistrer la configuration actuelle) est cochée, vous pouvez cocher **Mask passwords in the configuration file** (Masquer les mots de passe dans le fichier de configuration) afin de masquer tous les mots de passe de la configuration actuelle dans la copie de sauvegarde. Cependant, vous ne pouvez pas charger un fichier de configuration avec des mots de passe masqués à l'aide de la commande **Load Configuration** (Charger la configuration) ni de la commande **`loadconfig`** de l'interface de ligne de commande. Si le mode FIPS est activé, vous pouvez sélectionner **Encrypt passphrases in the Configuration Files** (Chiffrer les phrases secrètes dans les fichiers de configuration). Ces fichiers peuvent être rechargés. • Si l'option **Save current configuration** (Enregistrer la configuration actuelle) est cochée, vous pouvez entrer une ou plusieurs adresses de messagerie dans le champ **Email file to** (Envoyer le fichier à); une copie du fichier de configuration de sauvegarde est envoyée à chaque adresse. Séparez les valeurs multiples par des virgules.

Étape 3 Cliquez sur **Procéder**.

Si vous installez :

a) Soyez prêt à répondre aux invites pendant le processus.
b) À l'invite de fin, cliquez sur **Reboot Now** (Redémarrer maintenant).
c) Après environ 10 minutes, accédez à nouveau à l'appliance et connectez-vous.

Si vous pensez devoir redémarrer l'appliance pour résoudre un problème de mise à niveau, ne le faites pas avant qu'au moins 20 minutes se soient écoulées depuis le redémarrage.

Affichage de l'état, annulation ou suppression d'un téléchargement en arrière-plan

Étape 1 Choisissez **System Administration** > **System Upgrade** (Administration système > Mise à niveau du système).

Étape 2 Cliquez sur **Upgrade Options** (Options de mise à niveau).

Étape 3 Choisissez une option :

Destinataire	Faire ceci
Afficher l'état du téléchargement	Regardez au milieu de la page. Si aucun téléchargement n'est en cours et s'il n'y a aucun téléchargement terminé en attente d'installation, vous ne verrez aucune information sur l'état du téléchargement.
Annuler un téléchargement	Cliquez sur le bouton **Cancel Download** (Annuler le téléchargement) au milieu de la page. Cette option ne s'affiche que lorsqu'un téléchargement est en cours.
Supprimer un programme d'installation téléchargé	Cliquez sur le bouton **Delete File** (Supprimer le fichier) au milieu de la page. Cette option ne s'affiche que si un programme d'installation a été téléchargé.

Étape 4 (Facultatif) Affichez les journaux de mise à niveau.

Prochaine étape

Thèmes connexes

- Serveurs de mise à jour locaux et distants, à la page 617

Requêtes automatiques et manuelles de mise à jour et de mise à niveau

AsyncOS interroge périodiquement les serveurs de mise à jour pour connaître les nouvelles mises à jour pour tous les composants du service de sécurité, mais pas pour les nouvelles mises à niveau d'AsyncOS. Pour mettre à niveau AsyncOS, vous devez inviter manuellement AsyncOS à rechercher les mises à niveau disponibles. Vous pouvez également inviter manuellement AsyncOS à rechercher les mises à jour disponibles des services de sécurité. Pour en savoir plus, consultez Retour à une version antérieure d'AsyncOS pour le Web, on page 621.

Quand AsyncOS interroge un serveur de mise à jour pour une mise à jour ou une mise à niveau, il effectue les étapes suivantes :

1. Contacte le serveur de mise à jour.

   Cisco autorise les sources suivantes pour les serveurs de mise à jour :

   - **Serveurs de mise à jour Cisco.** Pour en savoir plus, consultez Mise à jour et mise à niveau à partir des serveurs de mise à jour Cisco, on page 617.
   - **Serveur local.** Pour en savoir plus, consultez Mise à niveau à partir d'un serveur local, on page 617.

2. Reçoit un fichier XML qui répertorie les mises à jour disponibles ou les versions de mise à niveau d'AsyncOS. Ce fichier XML est connu sous le nom de « fichier manifeste ».
3. Télécharge les fichiers image de mise à jour ou de mise à niveau.

Mise à jour manuelle des composants du service Security

Par défaut, chaque composant des services de sécurité reçoit régulièrement des mises à jour de ses tableaux de bases de données des serveurs de mises à jour de Cisco. Cependant, vous pouvez mettre à jour manuellement les tableaux de la base de données.

Note Certaines mises à jour sont disponibles sur demande à partir des pages de l'interface graphique utilisateur associées à la fonctionnalité.

Tip Affichez un enregistrement de l'activité de mise à jour dans le fichier journal du programme de mise à jour. Abonnez-vous au fichier journal du programme de mise à jour sur la page **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Note Les mises à jour en cours ne peuvent pas être interrompues. Toutes les mises à jour en cours doivent être terminées avant que de nouvelles modifications puissent être appliquées.

Étape 1 Choisissez **System Administration > Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour).

Étape 2 Cliquez sur **Edit Update Settings** (Modifier les paramètres de mise à jour).

Étape 3 Précisez l'emplacement des fichiers de mise à jour.

Étape 4 Lancez la mise à jour à l'aide de la touche de fonction Update Now (Mettre à jour maintenant) sur la page du composant située dans l'onglet Security Services (Services de sécurité). Par exemple, page Security Services > Web Reputation Filters (Services de sécurité > Filtres de réputation Web).

L'interface de commande en ligne et l'interface de l'application Web peuvent être lentes ou indisponibles pendant le processus de mise à jour.

Serveurs de mise à jour locaux et distants

Par défaut, AsyncOS contacte les serveurs de mise à jour Cisco pour obtenir les images de mise à jour et de mise à niveau et le fichier manifeste XML. Cependant, vous pouvez choisir de l'emplacement de téléchargement des images de mise à niveau et de mise à jour et du fichier manifeste. utilisation d'un serveur de mise à jour local pour les images ou le fichier manifeste pour l'une des raisons suivantes :

- **Vous avez plusieurs appliances à mettre à niveau simultanément.** Vous pouvez télécharger l'image de mise à niveau sur un serveur Web au sein de votre réseau et la diffuser sur toutes les appliances de votre réseau.
- **Les paramètres de votre pare-feu exigent des adresses IP statiques pour les serveurs de mise à jour Cisco.** Les serveurs de mise à jour Cisco utilisent des adresses IP dynamiques. Si vous avez des politiques de pare-feu strictes, vous devrez peut-être configurer un emplacement statique pour les mises à jour et les mises à niveau d'AsyncOS. Pour en savoir plus, consultez Configuration d'une adresse statique pour les serveurs de mise à jour Cisco, on page 617.

Note Les serveurs de mise à jour locaux ne reçoivent pas automatiquement les mises à jour du service de sécurité, mais uniquement les mises à niveau d'AsyncOS. Après avoir utilisé un serveur de mise à jour local pour la mise à niveau d'AsyncOS, modifiez les paramètres de mise à jour et de mise à niveau pour utiliser les serveurs de mise à jour Cisco afin que les services de sécurité se mettent à jour automatiquement.

Mise à jour et mise à niveau à partir des serveurs de mise à jour Cisco

Secure Web Appliance peut se connecter directement aux serveurs de mises à jour Cisco et télécharger les images de mise à niveau et les mises à jour des services de sécurité. Chaque appliance télécharge les mises à jour et les images de mise à niveau séparément.

Configuration d'une adresse statique pour les serveurs de mise à jour Cisco

Les serveurs de mise à jour Cisco utilisent des adresses IP dynamiques. Si vous avez des politiques de pare-feu strictes, vous devrez peut-être configurer un emplacement statique pour les mises à jour et les mises à niveau d'AsyncOS.

Étape 1 Communiquez avec l'assistance client de Cisco pour obtenir l'adresse URL statique.

Étape 2 Accédez à la page **System Administration** > **Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour), puis cliquez sur **Edit Update Settings** (Modifier les paramètres de mise à jour).

Étape 3 (Modifier les paramètres de mise à jour), dans la section « Update Servers (images) » [Serveurs de mise à jour (images)], choisissez **Local Update Servers** (Serveurs de mise à jour locaux) et entrez l'adresse URL statique reçue à l'étape 1.

Étape 4 Vérifiez que l'option Cisco Update Servers (Serveurs de mise à jour Cisco) est sélectionnée dans la section « Update Servers (list) » [Serveurs de mise à jour (liste)].

Étape 5 Envoyez et validez vos modifications.

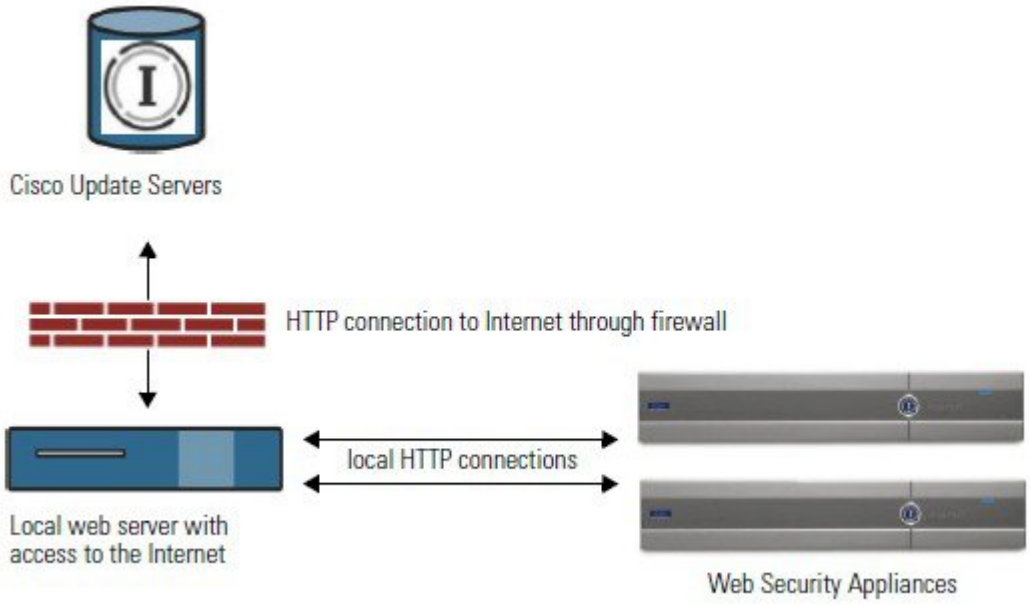
Mise à niveau à partir d'un serveur local

Secure Web Appliance peut télécharger les mises à niveau d'AsyncOS à partir d'un serveur de votre réseau au lieu d'obtenir des mises à niveau directement des serveurs de mise à jour Cisco. Cette fonctionnalité permet

de télécharger l'image de mise à niveau à partir de Cisco une seule fois, puis de la transmettre à tous les Secure Web Appliance de votre réseau.

La figure suivante montre comment les Secure Web Appliance télécharge les images de mise à niveau à partir de serveurs locaux.

Figure 11: Mise à niveau à partir d'un serveur local



Configuration matérielle et logicielle requise pour les serveurs locaux de mise à niveau

Pour *télécharger* les fichiers de mise à niveau AsyncOS, vous devez avoir un système dans votre réseau interne qui dispose d'un navigateur Web et d'un accès Internet aux serveurs de mise à jour Cisco.

Note Si vous devez configurer un paramètre de pare-feu pour autoriser l'accès HTTP à cette adresse, vous devez le faire en utilisant le nom DNS et non une adresse IP spécifique.

Pour *héberger* des fichiers de mise à niveau AsyncOS, un serveur du réseau interne doit avoir un serveur Web, comme Microsoft IIS (Internet Information Services) ou le serveur ouvert (Open Source) Apache, qui présente les caractéristiques suivantes :

- Prise en charge de l'affichage des noms de répertoires ou de fichiers dépassant 24 caractères.
- Navigation dans les répertoires activée.
- Configuré pour l'authentification anonyme (sans authentification) ou l'authentification de base (« simple »).
- Contient au moins 350 Mo d'espace disque libre pour chaque image de mise à niveau AsyncOS.

Configuration des mises à niveau à partir d'un serveur local

Note Cisco recommande de modifier les paramètres de mise à jour et de mise à niveau pour utiliser les serveurs de mise à jour Cisco (en utilisant des adresses dynamiques ou statiques) une fois la mise à niveau terminée pour garantir que les composants des services de sécurité continuent de se mettre à jour automatiquement.

Étape 1 Configurez un serveur local pour récupérer et distribuer servir les fichiers de mise à niveau.

Étape 2 Téléchargez le fichier de mise à niveau compressé.

À l'aide d'un navigateur sur le serveur local, accédez à la page http://updates.ironport.com/fetch_manifest.html pour télécharger un fichier compressé d'une image de mise à niveau. Pour télécharger l'image, entrez votre numéro de série (pour une appliance physique) ou VLN (pour une appliance virtuelle) et le numéro de version de l'appliance. Une liste des mises à niveau disponibles s'affichera ensuite. Cliquez sur la version de mise à niveau que vous souhaitez télécharger.

Étape 3 Décompressez le fichier compressé dans le répertoire racine sur le serveur local tout en préservant la structure de répertoires.

Étape 4 Configurez l'appliance pour utiliser le serveur local à l'aide de la page **System Administration > Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour) ou de la commande updateconfig.

Étape 5 Dans la page **System Administration > System Upgrade** (Administration système > Mise à niveau du système), cliquez sur **Availability Upgrades** (Mises à niveau disponibles) ou exécutez la commande upgrade.

Différences entre les méthodes de mise à niveau locale et à distance

Les différences suivantes s'appliquent lors de la mise à niveau d'AsyncOS à partir d'un serveur local plutôt que d'un serveur de mise à jour Cisco :

- La mise à niveau s'installe immédiatement *lors du téléchargement*.
- Une bannière s'affiche pendant 10 secondes au début du processus de mise à niveau. Pendant que cette bannière est affichée, vous avez la possibilité de taper Ctrl+C pour quitter le processus de mise à niveau avant le début du téléchargement.

Configuration des paramètres de mise à niveau et de mise à jour de services

Vous pouvez configurer la façon dont Secure Web Appliance télécharge les mises à jour des services de sécurité et les mises à niveau d'AsyncOS pour le Web. Par exemple, vous pouvez choisir l'interface réseau à utiliser lors du téléchargement des fichiers, configurer l'intervalle de mise à jour ou désactiver les mises à jour automatiques.

Étape 1 Choisissez **System Administration > Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour).

Étape 2 Cliquez sur **Edit Update Settings** (Modifier les paramètres de mise à jour).

Étape 3 Configurez les paramètres en vous référant aux informations suivantes :

Paramètres	Description
Automatic Updates (Mises à jour automatiques)	Choisissez si vous souhaitez activer les mises à jour automatiques des composants de sécurité. Si vous choisissez les mises à jour automatiques, saisissez l'intervalle de temps. La valeur par défaut est activée et l'intervalle de mise à jour est de 5 minutes.
Upgrade Notifications (Notifications de mise à niveau)	Choisissez si vous souhaitez afficher une notification en haut de l'interface Web quand une nouvelle mise à niveau vers AsyncOS est disponible. L'appliance affiche cette notification uniquement pour les administrateurs. Pour en savoir plus, consultez Mises à niveau et mises à jour d'AsyncOS pour le Web, on page 613.
Update Servers (list) [Mettre à jour les serveurs (liste)]	Permet de télécharger la liste des mises à niveau et mises à jour disponibles (fichier manifeste XML) à partir des serveurs de mises à jour Cisco ou d'un serveur Web local. Lorsque vous choisissez un serveur de mise à jour local, entrez le chemin d'accès complet au fichier manifeste XML pour obtenir la liste contenant le nom de fichier et le numéro de port du serveur. Si vous laissez le champ du port vide, AsyncOS utilise le port 80. Si le serveur exige une authentification, vous pouvez également saisir un nom d'utilisateur et une phrase secrète valides. • Pour obtenir le manifeste des appliances matérielles, tapez l'URL suivante : https://update-manifests.ironport.com • Pour obtenir le manifeste des appliances virtuelles, tapez l'URL suivante : https://update-manifests.sco.cisco.com
Update Servers (images) [Mettre à jour les serveurs (images)]	Permet de télécharger les images de mise à niveau et de mise à jour à partir des serveurs de mise à jour Cisco ou d'un serveur Web local. Lorsque vous choisissez un serveur de mise à jour local, entrez l'URL de base et le numéro de port du serveur. Si vous laissez le champ du port vide, AsyncOS utilise le port 80. Si le serveur exige une authentification, vous pouvez également saisir un nom d'utilisateur et une phrase secrète valides.
Routing Table (Tableau de routage)	Choisissez la table de routage de l'interface réseau à utiliser lorsque vous communiquez avec les serveurs de mise à jour.
Proxy Server (optional) [Serveur proxy (facultatif)]	S'il existe un serveur proxy en amont, qui exige une authentification, entrez les informations du serveur, le nom d'utilisateur et la phrase secrète ici.

Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Serveurs de mise à jour locaux et distants, on page 617
- Requêtes automatiques et manuelles de mise à jour et de mise à niveau, on page 615
- Mise à niveau et mise à jour d'AsyncOS et des composants du service Security, on page 613

Retour à une version antérieure d'AsyncOS pour le Web

AsyncOS pour le Web prend en charge la possibilité de rétablir une version précédente du système d'exploitation AsyncOS pour le Web pour les utilisations d'urgence.

Note Vous ne pouvez pas revenir à une version d'AsyncOS pour le Web antérieure à la version 7.5.

Le retour à une version antérieure d'AsyncOS sur les appliances virtuelles a une incidence sur la licence

Si vous revenez à AsyncOS 8.0, il n'y a pas de délai de grâce de 180 jours pendant lequel l'appliance traite les transactions Web sans fonctionnalités de sécurité. Les dates d'expiration des licences ne sont pas affectées.

Utilisation du fichier de configuration dans le processus de retour à une version antérieure

À partir de la version 7.5, lorsque vous mettez à niveau vers une version ultérieure, le processus de mise à niveau enregistre automatiquement la configuration actuelle du système dans un fichier sur Secure Web Appliance. (Cependant, Cisco recommande d'enregistrer manuellement le fichier de configuration sur un ordinateur local en tant que sauvegarde.) Cela permet à AsyncOS pour le Web de charger le fichier de configuration associé à la version antérieure après être revenu à la version antérieure. Cependant, lorsqu'il effectue une inversion, il utilise les paramètres réseau actuels pour l'interface de gestion.

Rétablissement de la version antérieure d'AsyncOS pour une appliance gérée par SMA

Vous pouvez rétablir AsyncOS pour le Web à partir de Secure Web Appliance. Toutefois, si Secure Web Appliance est géré par une appliance de gestion de la sécurité, tenez compte des règles et instructions suivantes :

- Lorsque les rapports centralisés sont activés sur Secure Web Appliance, AsyncOS pour le Web termine de transférer les données de rapport vers l'appliance de gestion de la sécurité avant de lancer le rétablissement de la version antérieure. Si le transfert des fichiers vers l'appliance de gestion de la sécurité est supérieur à 40 secondes, AsyncOS pour le Web vous invite à continuer à attendre pour transférer les fichiers, ou à poursuivre la restauration sans transférer tous les fichiers.
- Vous devez associer Secure Web Appliance à la configuration principale appropriée après le rétablissement. Sinon, le transfert d'une configuration de l'appliance de gestion de la sécurité vers Secure Web Appliance pourrait échouer.

Rétablissement d'une version antérieure d'AsyncOS pour le Web

Caution Rétablir le système d'exploitation sur un Secure Web Appliance est une action très destructrice, qui détruit tous les journaux de configuration et toutes les bases de données. Le rétablissement d'une version antérieure perturbe également le traitement du trafic Web jusqu'à ce que l'appliance soit reconfigurée. Selon la configuration initiale de Secure Web Appliance, cette action peut détruire la configuration réseau. Dans ce cas, vous aurez besoin d'un accès physique local à l'appliance après avoir effectué le rétablissement d'une version antérieure.

Caution La configuration des licences Smart ne peut pas être conservée si le système d'exploitation d'une appliance Cisco Secure Web Appliance est rétabli à la version antérieure avec les licences Smart activées. Lorsque vous êtes revenu à la version précédente d'AsyncOS, vous devez activer l'octroi de licences Smart et l'enregistrer sur le portail CSSM. Si l'option **Specific/Permanent License Reservation** (Réservation de licence permanente/spécifique) a été sélectionnée lors de l'activation de la licence logicielle Smart, il est recommandé de libérer les licences utilisées par l'appliance avant d'annuler l'opération et d'annuler l'enregistrement de l'appliance sur le portail CSSM. Vous pouvez contacter l'assistance de Cisco pour obtenir de l'aide, si les licences n'ont pas été publiées ou si l'enregistrement de l'appliance n'a pas été annulé avant l'opération de rétablissement d'une version antérieure.

Note Si des mises à jour de l'ensemble de catégories d'URL sont disponibles, elles seront appliquées après la restauration de la version antérieure d'AsyncOS.

Before you begin

- Communiquez avec le service d'assurance qualité de Cisco pour confirmer que vous pouvez effectuer le rétablissement d'une version antérieure prévu. (BS : il s'agit d'un résumé de la section Versions disponibles dans la rubrique d'origine. Ai demandé si cela est correct.)
- Sauvegardez les informations suivantes de Secure Web Appliance sur une machine distincte :
  - Fichier de configuration du système (avec phrase secrète non masquée)
  - Fichiers journaux que vous souhaitez conserver.
  - Rapports que vous souhaitez conserver.
  - Pages de notification personnalisées de l'utilisateur final stockées sur l'appliance.
  - Fichiers PAC stockés sur l'appliance.

Étape 1 Connectez-vous à l'interface de ligne de commande de l'appliance dont vous voulez rétablir une version antérieure.

Note Lorsque vous exécutez la commande `revert` à l'étape suivante, plusieurs invites d'avertissement sont émises. Une fois ces avertissements acceptés, le rétablissement de la version antérieure est exécuté immédiatement. Par conséquent, ne commencez pas le processus de restauration avant d'avoir terminé les étapes préalables au rétablissement de la version antérieure.

Étape 2 Saisissez la commande `revert`.

Étape 3 Confirmez deux fois que vous souhaitez poursuivre le rétablissement de la version antérieure.

Étape 4 Choisissez l'une des versions disponibles auquel revenir.

L'appliance redémarre deux fois.

Note Le processus de rétablissement d'une version antérieure prend du temps. Cela peut prendre de quinze à vingt minutes avant que la restauration ne soit terminée et que l'accès à l'appliance par la console soit à nouveau disponible.

L'appliance devrait maintenant fonctionner avec la version sélectionnée d'AsyncOS pour le Web. Vous pouvez accéder à l'interface Web à partir d'un navigateur Web.

Supervision de l'intégrité et de l'état du système à l'aide de SNMP

Le système d'exploitation AsyncOS prend en charge la supervision de l'état du système par le biais de SNMP (Simple Network Management Protocol). (Pour en savoir plus sur SNMP, consultez les RFC 1065, 1066 et 1067.)

Prenez note :

- SNMP est **désactivé** par défaut.
- Les opérations SET de SNMP (configuration) ne sont pas mises en œuvre.
- AsyncOS prend en charge SNMPv1, v2 et v3. Pour en savoir plus sur SNMPv3, consultez les RFC 2571-2575.
- L'authentification et le chiffrement des messages sont obligatoires lors de l'activation de SNMPv3. Les phrases secrètes pour l'authentification et le chiffrement doivent être différentes. L'algorithme de chiffrement peut être AES (recommandé) ou DES. L'algorithme d'authentification peut être SHA-1 (recommandé) ou MD5. La commande snmpconfig « se souviendra » de vos phrases secrètes la prochaine fois que vous l'exécuterez.
- Le nom d'utilisateur SNMPv3 est : v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- Si vous utilisez uniquement SNMPv1 ou SNMPv2, vous devez définir un identifiant de communauté. L'identifiant de communauté ne prend pas la valeur `public` par défaut.
- Pour SNMPv1 et SNMPv2, vous devez spécifier un réseau à partir duquel les demandes SNMP GET sont acceptées.
- Pour utiliser des interruptions, un gestionnaire SNMP (non inclus dans AsyncOS) doit être en cours d'exécution et son adresse IP doit être saisie comme cible d'interruption. (Vous pouvez utiliser un nom d'hôte, mais si vous le faites, les interruptions ne fonctionneront que si le DNS est opérationnel.)

Fichiers MIB

Les fichiers MIB sont disponibles à l'adresse suivante http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Utilisez la dernière version de chaque fichier MIB.

Il existe plusieurs fichiers MIB :

- asyncoswebsecurityappliance-mib.txt : description compatible avec SNMPv2 de la MIB d'entreprise pour les Secure Web Appliance.
- ASYNCOS-MAIL-MIB.txt : description compatible avec SNMPv2 de la MIB d'entreprise pour les appliances de sécurité de la messagerie.
- IRONPORT-SMI.txt : ce fichier de « structure des informations de gestion » définit le rôle d'asyncoswebsecurityappliance-mib.

Cette version met en œuvre un sous-ensemble en lecture seule de MIB-II, comme défini dans les RFC 1213 et 1907.

Consultez https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html pour en savoir plus sur la supervision de l'utilisation du processeur sur l'appliance à l'aide de SNMP.

Activation et configuration de la supervision SNMP

Pour configurer SNMP afin de recueillir des informations sur l'état du système pour l'appliance, utilisez la commande snmpconfig dans l'interface de ligne de commande (CLI). Une fois que vous avez choisi et configuré les valeurs d'une interface, l'appliance répond aux demandes SNMPv3 GET.

Lorsque vous utilisez la supervision SNMP, gardez les points suivants à l'esprit :

- Ces demandes de version 3 doivent inclure une phrase secrète correspondante.
- Par défaut, les demandes des versions 1 et 2 sont rejetées.
- Si elle est activée, les demandes des versions 1 et 2 doivent avoir un identifiant de communauté correspondant.

Objets matériels

Des capteurs matériels conformes à la spécification IPMI (Intellect Platform Management Interface Precision) transmettent des renseignements comme la température, la vitesse du ventilateur et l'état du bloc d'alimentation.

Pour déterminer les objets matériels disponibles pour la supervision (par exemple, le nombre de ventilateurs ou la plage de températures de fonctionnement), consultez le guide du matériel pour votre modèle d'appliance.

Thèmes connexes

- Documentation, on page 695

Interruptions SNMP

SNMP permet d'envoyer des interruptions, ou des notifications, pour informer une application d'administration qu'une ou plusieurs conditions sont satisfaites. Les interruptions sont des paquets réseau qui contiennent des

données relatives à un composant du système qui envoie l'interruption. Les interruptions sont générées quand une condition est remplie sur l'agent SNMP (dans ce cas, Cisco Secure Web Appliance). Une fois la condition remplie, l'agent SNMP forme un paquet SNMP et l'envoie à l'hôte qui exécute le logiciel de la console de gestion SNMP.

Vous pouvez configurer les interruptions SNMP (activer ou désactiver des interruptions particulières) lorsque vous activez SNMP pour une interface.

Pour spécifier plusieurs cibles d'interruption : lorsque vous êtes invité à saisir la cible d'interruption, vous pouvez entrer jusqu'à 10 adresses IP séparées par des virgules.

Thèmes connexes

- À propos de l'interruption SNMP connectivityFailure , on page 625

À propos de l'interruption SNMP connectivityFailure

L'interruption connectivityFailure est destinée à surveiller la connexion de votre appliance à Internet. Pour ce faire, il tente de se connecter et envoie une requête HTTP GET à un seul serveur externe toutes les 5 à 7 secondes. Par défaut, l'URL surveillée est `downloads.ironport.com` sur le port 80.

Pour modifier l'URL ou le port surveillés, exécutez la commande `snmpconfig` et activez l'interruption connecivityFailure, même si elle est déjà activée. Vous verrez une invite pour modifier l'URL.

Tip Pour simuler des interruptions connectivityFailure, vous pouvez utiliser la commande d'interface de ligne de commande `dnsconfig` pour saisir un serveur DNS qui ne fonctionne pas. Les recherches pour downloads.ironport.com vont échouer, et des interruptions seront envoyées toutes les 5 à 7 secondes. Assurez-vous de remplacer le serveur DNS par un serveur qui fonctionne après avoir terminé votre test.

Exemple d'interface de ligne de commande : snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2
```

```
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>

Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y

Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y

Enter number or numbers of traps to enable.  Separate multiple numbers with
```

```
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```

Dérivation du trafic Web

Avant de commencer : l'activation de la fonction Web Traffic Tap (Dérivation du trafic Web) réduira la capacité de traitement des transactions (demandes par seconde) de l'appliance, car cette dernière aura besoin de cycles de processeur et de mémoire supplémentaires pour copier les messages dans l'interface de dérivation.

Remarque Pour réduire l'impact sur les performances de la fonctionnalité Web Traffic Tap (Dérivation du trafic Web), réduisez le volume de trafic dérivé en définissant des politiques de dérivation du trafic Web appropriées.

Cette fonctionnalité n'est pas prise en charge sur Amazon Web Services (AWS)

La fonctionnalité Web Traffic Tap (Dérivation du trafic Web) vous permet de dériver le trafic Web HTTP et HTTPS qui traverse l'appliance et de le copier dans une interface Secure Web Appliance en ligne avec le trafic de données en temps réel. Vous pouvez sélectionner l'interface Secure Web Appliance à laquelle les données de trafic dérivées sont envoyées. Si le trafic dérivé inclut des données HTTPS, l'appliance les déchiffre en fonction des politiques de déchiffrement avant de les envoyer à l'interface de dérivation. Consultez Politiques de déchiffrement , à la page 281.

L'interface de dérivation sélectionnée doit être directement connectée à un périphérique de sécurité externe à des fins d'analyse, d'investigation et d'archivage. Sinon, elle peut être connectée à un commutateur L2 sur un VLAN dédié.

Remarque Le trafic reflété sur l'interface de dérivation est diffusé sur la couche Ethernet et n'est pas routable sur IP. Par conséquent, un VLAN dédié est requis s'il est connecté à un commutateur de couche 2.

Cette fonctionnalité vous permet également de définir des politiques de dérivation du trafic Web. En fonction de ces filtres de politique définis par le client, l'appliance reflète le trafic Web disponible pour le périphérique de sécurité externe. La fonctionnalité Web Traffic Tap (Dérivation du trafic Web) offre une visibilité sur le trafic HTTPS.

Le terme « dérivation » fait référence à la reconstitution de flux TCP (Transmission Control Protocol) complets comme s'ils se produisaient entre un client et un serveur directement connectés.

Les Secure Web Appliance virtuels prennent en charge la fonctionnalité Web Traffic Tap (Dérivation du trafic Web).

Remarque L'inspection du trafic SSL peut être soumise aux politiques de l'entreprise et/ou à la législation nationale. Cisco n'est responsable d'aucune obligation légale et il est de votre seule responsabilité de vous assurer que votre utilisation de la fonctionnalité Web Traffic Tap (Dérivation du trafic Web) sur Secure Web Appliance est conforme à ces exigences légales ou à ces politiques.

Vous devez effectuer les procédures suivantes pour dériver le trafic Web à l'aide de l'appliance :

1. Activer la fonctionnalité Web Traffic Tap (Dérivation du trafic Web)
2. Configurer les politiques de dérivation du trafic Web

Thèmes connexes

- Activation de la dérivation du trafic Web, à la page 628
- Configuration des politiques de dérivation du trafic Web, à la page 629

Activation de la dérivation du trafic Web

Avant de commencer

La fonctionnalité Web Traffic Tap (Dérivation du trafic Web) est désactivée par défaut. Vous devez activer cette fonctionnalité avant de définir les politiques de dérivation du trafic Web en sélectionnant **Web Security Manager** > **Web Traffic Tap Policies** (Politiques de dérivation du trafic Web).

Remarque Des politiques de déchiffrement doivent être définies afin de dériver les transactions HTTPS. Consultez Politiques de déchiffrement , à la page 281.

Étape 1 Choisissez **Network** > **Web Traffic Tap** (Réseau > Dérivation du trafic Web).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la page Edit Web Traffic Tap (Modifier la dérivation du trafic Web), cochez la case **Enable** (Activer) pour activer la fonction Web Traffic Tap (Dérivation du trafic Web).

Remarque Pour désactiver la fonctionnalité Web Traffic Tap feature, (Dérivation du trafic Web), décochez la case **Enable** (Activer). Si vous désactivez la fonctionnalité Web Traffic Tap (Dérivation du trafic Web), vous ne pourrez pas afficher ni modifier les politiques relatives à la dérivation du trafic Web. Vous devez réactiver cette fonction pour afficher et modifier les politiques.

Étape 4 Dans la liste déroulante Tap Interface (Interface de dérivation), choisissez l'interface Secure Web Appliance vers laquelle les données du trafic déviées sont envoyées. Les options d'interface sont P1, P2, T1 et T2. Consultez Connecter l'appliance, à la page 13 pour en savoir plus sur les interfaces.

Remarque L'interface de dérivation sélectionnée doit être directement connectée à un périphérique de sécurité externe à des fins d'analyse, d'investigation et d'archivage. Sinon, elle peut être connectée à un commutateur L2 sur un VLAN dédié. L'interface de dérivation choisie doit être connectée et son état doit être actif; sinon, la mise en miroir du trafic dévié échouera.

Étape 5 Cliquez sur **Submit** (Envoyer) et validez vos modifications.

Configuration des politiques de dérivation du trafic Web

Étape 1 Choisissez **Web Security Manager** > **Web Traffic Tap Policies** (Politiques de dérivation du trafic Web).

Étape 2 Cliquez sur **Add Policy** (Ajouter une politique).

Suivez les instructions à la section Création d'une politique , à la page 253 pour ajouter une nouvelle politique de dérivation du trafic Web.

Remarque Une politique de dérivation du trafic globale sans dérivation définie est disponible par défaut dans la page Web Traffic Tap Policies (Politiques de dérivation du trafic Web) [**Web Security Manager** > **Web Traffic Tap Policies** (Web Security Manager > Politiques de dérivation du trafic Web)].

Étape 3 Développez la section avancée de la zone de définition de membre de politique pour ajouter les critères d'appartenance au groupe supplémentaires suivants pour la dérivation du trafic Web.

- Protocols (Protocoles) : choisissez les protocoles HTTP, HTTPS ou les deux pour créer une politique de déviation du trafic Web.

  Remarque Vous devez définir la politique de déchiffrement correspondante [**Web Security Manager** > **Decryption Policies** (Web Security Manager > Politiques de déchiffrement)] afin de dériver le trafic HTTPS.

  Les politiques de dérivation du trafic Web ne prennent pas en charge les protocoles natifs FTP et SOCKS.

- Subnets (Sous-réseaux)

- URL Categories (Catégories d'URL) : définissez les catégories de filtrage d'URL sur **Tap** (Dérivation) **No Tap** (Sans dérivation), selon vos besoins. Pour définir le dérivateur de trafic pour les URL non classées, choisissez **Tap** (Dérivation) dans la liste déroulante des URL non classées et cliquez sur **Submit** (Envoyer).
- User Agents (Agents utilisateur)

Consultez Création d'une politique , à la page 253 pour en savoir plus sur la définition de critères d'appartenance à un groupe supplémentaires.

Remarque Le trafic que vous souhaitez dériver doit satisfaire à toutes les conditions de filtre que vous avez définies pour la politique de dérivation du trafic Web.

Vous pouvez également ajouter des catégories d'URL à partir du tableau de filtrage d'URL en sélectionnant **Web Security Manager** > **Web Traffic Tap Policies** (Web Security Manager > Politiques de dérivation du trafic Web).

Remarque Si vous avez déjà ajouté les catégories d'URL dans la section Advanced (Avancé), vous ne verrez que les catégories d'URL répertoriées dans le tableau de filtrage d'URL [**Web Security Manager** > **Web Traffic Tap Policies** (Web Security Manager > Politiques de dérivation du trafic Web)].

Consultez Ordre des politiques, à la page 252 pour connaître l'ordre des politiques de dérivation du trafic Web.

Configuration du protocole HTTP 2.0

La version 14.0 de Cisco AsyncOS prend en charge HTTP 2.0 pour les demandes et les réponses Web sur TLS.

HTTP 2.0 pour les requêtes et réponses Web sur TLS. La prise en charge de HTTP 2.0 nécessite une négociation basée sur TLS ALPN, disponible uniquement à partir de la version TLS 1.2.

Dans cette version, HTTPS 2.0 n'est pas pris en charge pour les fonctionnalités suivantes :

- Dérivation du trafic Web
- DLP externe
- Bande passante globale et bande passante de l'application

Remarque Par défaut, la fonctionnalité HTTP 2.0 est désactivée et utilisez la commande de l'interface de ligne de commande HTTP 2 pour l'activer.

La fonctionnalité HTTP 2.0 prend en charge :

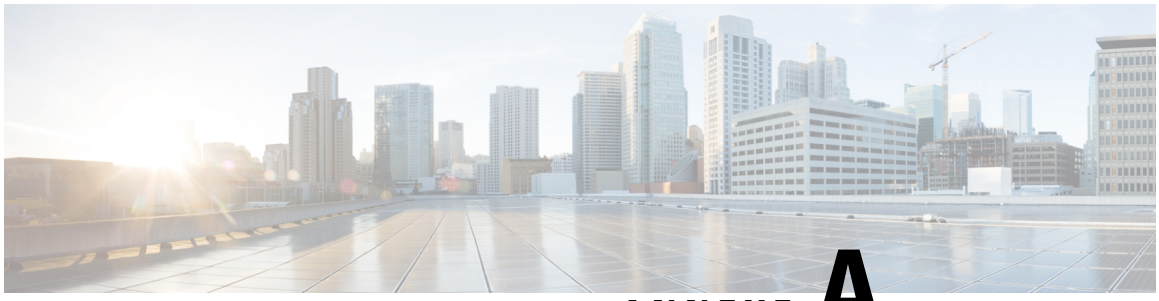
- Un maximum de 4096 sessions simultanées et 128 flux simultanés
- Tous les protocoles HTTP dans l'ALPN et un maximum de sept protocoles dans l'ALPN annoncé.
- Une taille d'en-tête maximale de 16 Ko.

Remarque CONNECT pour le proxy explicite dans la version 2.0 commence également par HTTP 1.1.

Une nouvelle commande de l'interface de ligne de commande `HTTP2` est introduite pour activer ou désactiver les configurations HTTP 2.0. Voir les commandes d'interface de ligne de commande Commandes de l'interface de ligne de commande Secure Web Appliance.

Vous ne pouvez pas activer ou désactiver HTTP 2.0 et restreindre le domaine pour HTTP 2.0 à l'aide de l'interface utilisateur Web de l'appliance. La configuration de HTTP 2.0 n'est pas prise en charge par Cisco Secure Email and Web Manager (appliances de gestion de la sécurité du contenu Cisco).

- Lorsque l'URL échoue à la fois dans les listes d'exceptions HTTP 2 et dans les catégories d'URL d'intercommunication, HTTP 2 prévaut sur l'intercommunication.
- La journalisation ALPN n'est pas cohérente pour les catégories d'URL de liaison.



ANNEXE A

Dépannage

Cette rubrique contient les sections suivantes :

Bonnes pratiques en matière de résolution des problèmes d'ordre général

Configurez vos journaux d'accès pour inclure les champs personnalisés suivants :

%u, %g, %m, %k, %L (ces valeurs sont sensibles à la casse.)

Pour une description de ces champs, consultez Spécificateurs de format des journaux d'accès et champs des fichiers journaux W3C, on page 529.

Pour les instructions de configuration, consultez Personnalisation des journaux d'accès, on page 523 et Ajout et modification d'abonnements aux journaux, on page 491.

Problèmes du mode FIPS

Consultez les rubriques suivantes si vous rencontrez des problèmes de chiffrement et de certificat après avoir mis à niveau votre Secure Web Appliance vers AsyncOS 10.5 et activé le mode FIPS et le chiffrement CSP.

- Chiffrement CSP, à la page 634
- Validation des certificats, à la page 634

Chiffrement CSP

Pour une fonctionnalité qui était opérante avant que vous activiez le chiffrement CSP en mode FIPS, mais qui ne fonctionne pas après l'activation du chiffrement, déterminez si le chiffrement CSP est le problème. Désactivez le chiffrement CSP et le mode FIPS, puis testez la fonction. Si cela fonctionne, activez le mode FIPS et testez-le à nouveau. Si cela fonctionne, activez le chiffrement CSP et testez-le à nouveau. Consultez Activation ou désactivation du mode FIPS , à la page 605.

Validation des certificats

Les certificats qui ont été acceptés par votre Secure Web Appliance avant la mise à niveau vers AsyncOS 10.5 peuvent être rejetés lorsqu'ils sont à nouveau chargés, quelle que soit la méthode de chargement. (C'est-à-dire par le biais des pages de l'interface utilisateur telles que le proxy HTTPS, la gestion des certificats, le fournisseur d'identité pour SaaS, la configuration ISE, la configuration de l'authentification ou la commande de l'interface de ligne de commande `certconfig`.)

Assurez-vous que les autorités de certification signataires du certificat ont été ajoutées en tant « qu'autorités de certification approuvées personnalisées » dans la page Certificate Management (Gestion des certificats) [Network > Certificate Management (Réseau > Gestion des certificats)]. Un certificat ne peut pas être téléchargé vers le Secure Web Appliance si le chemin d'accès complet au certificat n'est pas fiable.

En outre, lors du rechargement d'une configuration plus ancienne, il est probable que les certificats inclus ne seront pas fiables et que le rechargement échoue. Assurez-vous que ces certificats sont remplacés lors du chargement de la configuration enregistrée.

Remarque Tous les échecs de validation de certificat sont consignés dans les journaux d'audit (`/data/pub/audit_logs/audit_log.current`).

Problèmes d'authentification

- Outils de résolution de problèmes pour les problèmes d'authentification , on page 635
- L'échec de l'authentification a une incidence sur les opérations normales, on page 635

- Problèmes relatifs au protocole LDAP, on page 635
- Problèmes d'authentification de base, on page 636
- Problèmes de connexion unique, on page 636
- Voir également :
  - Bonnes pratiques en matière de résolution des problèmes d'ordre général, on page 633
  - Les demandes HTTPS et FTP via HTTP correspondent uniquement aux politiques d'accès qui ne nécessitent pas d'authentification, on page 652
  - Impossible d'accéder aux URL qui ne prennent pas en charge l'authentification, on page 658
  - Échec des demandes du client au proxy en amont, on page 660

Outils de résolution de problèmes pour les problèmes d'authentification

KerbTray ou klist (qui font tous deux partie du Kit de ressources du serveur Windows) pour l'affichage et la purge d'un cache de ticket Kerberos. Explorateur Active Directory pour l'affichage et la modification d'un répertoire Active Directory Wireshark est un analyseur de paquets que vous pouvez utiliser pour le dépannage de réseau.

L'échec de l'authentification a une incidence sur les opérations normales

Lorsque certains agents utilisateurs ou certaines applications ne parviennent pas à s'authentifier et se voir refuser l'accès, ils envoient des demandes à plusieurs reprises à Secure Web Appliance, qui envoie à son tour des demandes aux serveurs Active Directory avec les informations d'identification de l'ordinateur, parfois au point d'affecter les opérations normales.

Pour de meilleurs résultats, contournez l'authentification à l'aide de ces agents utilisateurs. Consultez Contournement de l'authentification avec des agents utilisateur problématiques , on page 142.

Problèmes relatifs au protocole LDAP

- Échec d'authentification de l'utilisateur LDAP en raison du protocole NTLMSSP, on page 635
- Échec de l'authentification LDAP en raison du renvoi au protocole LDAP, on page 636

Échec d'authentification de l'utilisateur LDAP en raison du protocole NTLMSSP

Les serveurs LDAP ne prennent pas en charge NTLMSSP. Certaines applications clientes, comme Internet Explorer, choisissent toujours NTLMSSP lorsqu'elles ont le choix entre NTLMSSP et Basic (Basique). Si toutes les conditions suivantes sont satisfaites, l'authentification de l'utilisateur échouera :

- L'utilisateur existe uniquement dans le domaine LDAP.
- Le profil d'identification utilise une séquence qui contient à la fois les domaines LDAP et NTLM.
- Le profil d'identification utilise le schéma d'authentification Basic ou NTLMSSP.
- Un utilisateur envoie une demande à partir d'une application qui choisit NTLMSSP au lieu de Basic.

Reconfigurez le profil d'identification, le domaine d'authentification ou l'application de sorte qu'au moins une des conditions ci-dessus soit fausse.

Échec de l'authentification LDAP en raison du renvoi au protocole LDAP

L'authentification LDAP échoue lorsque toutes les conditions suivantes sont remplies :

- Le domaine d'authentification LDAP utilise un serveur Active Directory.
- Le serveur Active Directory utilise une recommandation LDAP vers un autre serveur d'authentification.
- Le serveur d'authentification désigné n'est pas disponible pour Secure Web Appliance.

Solutions :

- Indiquez le serveur de catalogue global (le port par défaut est 3268) dans la forêt Active Directory lorsque vous configurez le domaine d'authentification LDAP dans l'appliance.
- Utilisez la commande d'interface de ligne de commande `advancedproxyconfig` > `authentication` pour désactiver les recommandations LDAP. Les recommandations LDAP sont désactivées par défaut.

Problèmes d'authentification de base

- Échec de l'authentification de base, on page 636

Problèmes connexes

- Le proxy en amont ne reçoit pas les informations d'authentification de base, on page 659

Échec de l'authentification de base

AsyncOS pour le Web prend uniquement en charge les caractères ASCII 7 bits pour les phrases secrètes lors de l'utilisation du schéma d'authentification de base. L'authentification de base échoue lorsque la phrase secrète contient des caractères qui ne sont pas des caractères ASCII 7 bits.

Problèmes de connexion unique

- Utilisateurs invités par erreur à fournir des informations d'authentification, on page 636

Utilisateurs invités par erreur à fournir des informations d'authentification

L'authentification NTLM ne fonctionne pas dans certains cas lorsque Secure Web Appliance est connecté à un périphérique compatible avec WCCP v2. Lorsqu'un utilisateur effectue une demande avec une version hautement verrouillée d'Internet Explorer qui n'effectue pas l'authentification NTLM transparente correctement et que l'appliance est connectée à un périphérique compatible avec WCCP v2, le navigateur utilise par défaut l'authentification de base. Ainsi, les utilisateurs sont invités à saisir leurs informations d'authentification alors qu'ils ne devraient pas les recevoir.

Solution de rechange

Dans Internet Explorer, ajoutez le nom d'hôte de redirection Secure Web Appliance à la liste des sites approuvés dans la zone Local Intranet (Intranet local) [Tools > Internet Options > Security tab (Outils > Options Internet > onglet Sécurité)].

Problèmes d'objets bloqués

Certains fichiers Microsoft Office ne sont pas bloqués

Lorsque vous bloquez des fichiers Microsoft Office dans la section Block Object Type (Bloquer le type d'objet), il est possible que certains fichiers Microsoft Office ne soient pas bloqués.

Si vous devez bloquer tous les fichiers Microsoft Office, ajoutez **application/x-ole** dans le champ Block Personal MIME Types (Bloquer les types MIME personnalisés). Cependant, le blocage de ce type MIME personnalisé bloque également tous les types de formats d'objets composés Microsoft, tels que les fichiers Visio et certaines applications tierces.

Le blocage des types d'objets exécutables DOS bloque les mises à jour pour Windows OneCare

Lorsque vous configurez Secure Web Appliance pour bloquer les types d'objets exécutables DOS, l'appliance bloque également les mises à jour pour Windows OneCare.

Problèmes de navigateur

WPAD ne fonctionne pas avec Firefox

Il est possible que les navigateurs Firefox ne prennent pas en charge la recherche DHCP avec WPAD. Pour obtenir les informations les plus récentes, consultez `https://bugzilla.mozilla.org/show_bug.cgi?id=356831`.

Pour utiliser Firefox (ou tout autre navigateur qui ne prend pas en charge DHCP) avec WPAD lorsque le fichier PAC est hébergé sur Secure Web Appliance, configurez l'appliance de manière à servir le fichier PAC par le port 80.

Étape 1 Choisissez **Security Services > Web Proxy** (Services de sécurité > Proxy Web) et supprimez le port 80 du champ **HTTP Ports to Proxy** (Ports HTTP vers proxy).

Étape 2 Utilisez le port 80 comme port du serveur PAC lorsque vous chargez le fichier sur l'appliance.

Étape 3 Si des navigateurs sont configurés manuellement pour pointer vers le proxy Web sur le port 80, reconfigurez ces navigateurs afin qu'ils pointent vers un autre port dans le champ HTTP Ports to Proxy (Ports HTTP vers proxy).

Étape 4 Modifiez toutes références au port 80 dans les fichiers PAC.

Problèmes de DNS

Alerte : Échec du démarrage du cache DNS

Si une alerte contenant le message « Failed to bootstrap the DNS cache » (Échec du démarrage du cache DNS) est générée au redémarrage d'une appliance, cela signifie que le système n'a pas pu contacter ses serveurs DNS principaux. Cela peut se produire au démarrage si le sous-système DNS est mis en ligne avant que la connectivité réseau ne soit établie. Si ce message s'affiche à d'autres stades, cela peut indiquer des problèmes de réseau ou que la configuration DNS ne pointe pas vers un serveur valide.

Problèmes de basculement

Configuration de basculement incorrecte

Une mauvaise configuration des groupes de basculement peut entraîner la création de plusieurs périphériques principaux ou d'autres problèmes de basculement. Diagnostiquez les problèmes de basculement à l'aide de la sous-commande `testfailovergroup` de la commande d'interface de ligne de commande `failoverconfig`.

Par exemple :

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: PRIMARY
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

Problèmes de basculement sur les appliances virtuelles

Pour les déploiements sur des appliances virtuelles, assurez-vous d'avoir configuré l'interface/le commutateur virtuel sur l'hyperviseur pour utiliser le mode promiscuité.

Clés de fonctionnalité expirées

Si la clé de fonctionnalité à laquelle vous essayez d'accéder (par l'interface Web) a expiré, communiquez avec votre représentant Cisco ou avec le service d'assistance.

Problèmes de FTP

Les catégories d'URL ne bloquent pas certains sites FTP

Lorsqu'une requête FTP native est redirigée vers le proxy FTP de manière transparente, elle ne contient aucune information de nom d'hôte pour le serveur FTP, seulement son adresse IP. C'est pourquoi certaines catégories d'URL et certains filtres de réputation Web prédéfinis qui n'ont que des informations de nom d'hôte ne correspondront pas aux demandes FTP natives, même si les demandes sont destinées à ces serveurs. Si vous souhaitez bloquer l'accès à ces sites, vous devez créer des catégories d'URL personnalisées en utilisant leurs adresses IP.

Déconnexion des transferts FTP volumineux

Si la connexion entre le proxy FTP et le serveur FTP est lente, le chargement d'un fichier volumineux peut prendre beaucoup de temps, en particulier lorsque les filtres de sécurité des données Cisco sont activés. Cela peut entraîner l'expiration du délai d'expiration du client FTP avant que le proxy FTP télécharge le fichier entier et vous pourriez obtenir un avis d'échec de transaction. La transaction n'échoue pas, cependant, mais continue en arrière-plan et sera terminée par le proxy FTP.

Vous pouvez contourner ce problème en augmentant la valeur du délai d'inactivité appropriée sur le client FTP.

Le fichier de zéro octet apparaît sur les serveurs FTP après le chargement du fichier

Les clients FTP créent un fichier de zéro octet sur les serveurs FTP lorsque le mandataire FTP bloque un téléchargement en raison de l'analyse de protection contre les programmes malveillants sortant.

Navigateur Chrome non détecté en tant qu'agent utilisateur dans les requêtes FTP via HTTP

Les navigateurs Chrome n'incluent pas de chaîne user-agent dans les demandes FTP-sur-HTTP ; par conséquent, Chrome ne peut pas être détecté en tant qu'agent utilisateur dans ces demandes.

Problèmes de vitesse de chargement/téléchargement

Le Secure Web Appliance est conçu pour gérer des milliers de connexions de clients et de serveur en parallèle, et la taille des tampons d'envoi et de réception est configurée pour offrir des performances optimales, sans sacrifier la stabilité. En général, l'utilisation réelle correspond au trafic de navigation, qui consiste en de nombreuses connexions de courte durée pour lesquelles nous avons des données de direction de réception de paquets (RPS) et de direction de flux de réception (RFS), et pour lesquelles Secure Web Appliance a été optimisé.

Cependant, il se peut que vous rencontriez parfois une réduction notable des vitesses de chargement ou de téléchargement; Par exemple, lors du transfert de fichiers volumineux par un proxy. Par exemple, en supposant une ligne à 10 Mbit/s, le téléchargement d'un fichier de 100 Mo qui passe par un Secure Web Appliance peut être environ sept à huit fois plus lent que le téléchargement du fichier directement à partir du serveur.

Dans les environnements inhabituels qui comprennent une proportion plus élevée de transferts de fichiers volumineux, vous pouvez utiliser la commande `networktuning` pour augmenter la taille de la mémoire tampon d'envoi et de réception afin de résoudre ce problème, mais cela peut également épuiser la mémoire réseau et affecter la stabilité du système. Consultez Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671 pour en savoir plus sur la commande `networktuning`.

Caution Faites preuve de prudence lorsque vous modifiez les points de contrôle de la mémoire tampon de réception et d'envoi du protocole TCP et d'autres paramètres de la mémoire tampon TCP. Utilisez la commande `networktuning` uniquement si vous en comprenez les ramifications.

Pour configurer la taille de la mémoire tampon dans `networktuning`, assurez-vous d'avoir activé les options d'envoi et de réception automatiques fournies dans `networktuning`.

Voici des exemples d'utilisation de la commande `networktuning` sur deux appliances différentes :

Sur un S380

```
networktuning
sendspace = 131072
recvspace = 131072
send-auto = 1 [Remember to disable miscellaneous > advancedproxy > send buf auto tuning]
recv-auto = 1 [Remember to disable miscellaneous > advancedproxy > recv buf auto tuning]
mbuf clusters = 98304 * (X/Y)  where is X is RAM in GBs on the system and Y is 4GB.
sendbuf-max = 1048576
recvbuf-max = 1048576
```

Questions

Quels sont ces paramètres?

Secure Web Appliance comprend plusieurs tampons et algorithmes d'optimisation qui peuvent être modifiés pour des besoins spécifiques. Les tailles des tampons sont optimisées à l'origine pour s'adapter aux scénarios

de déploiement « les plus courants ». Cependant, des tailles de tampon plus grandes peuvent être utilisées lorsque des performances par connexion plus rapides sont nécessaires, mais notez que l'utilisation globale de la mémoire augmentera. Par conséquent, l'augmentation de la taille de la mémoire tampon doit correspondre à la mémoire disponible sur le système. Les variables d'espace d'envoi et de réception contrôlent la taille des tampons disponibles pour le stockage des données pour la communication sur une interface de connexion. Les options send- et received-auto sont utilisées pour activer et désactiver la mise à l'échelle dynamique des tailles de fenêtre TCP d'envoi et de réception. (Ces paramètres sont appliqués dans le noyau de FreeBSD.)

Comment ces exemples de valeurs ont-ils été déterminés?

Nous avons testé différents ensembles de valeurs sur le réseau d'un client, où ce « problème » a été observé, et nous avons « rapprocher » ces valeurs. Nous avons ensuite testé ces modifications dans un contexte de stabilité et d'augmentation des performances dans nos laboratoires. Vous êtes libre d'utiliser des valeurs autres que celles-ci à vos propres risques.

Pourquoi ces valeurs ne sont-elles pas celles par défaut?

Comme mentionné, par défaut, Secure Web Appliance est optimisé pour les déploiements les plus courants et fonctionne dans un très grand nombre d'emplacements sans problème de performance par connexion. Les modifications décrites ici n'augmenteront pas les nombres de RPS et pourraient en fait les faire disparaître.

Problèmes matériels

Redémarrage bref de l'appliance

Important! Si vous devez éteindre et rallumer votre appliance x80 ou x90, attendez au moins 20 minutes que l'appliance se rallume (tous les voyants DEL sont verts) avant d'appuyer sur le bouton d'alimentation.

Indicateurs d'intégrité et d'état de l'appliance

Les voyants DEL à l'avant ou à l'arrière de votre appliance matérielle indiquent l'état de fonctionnement de votre appliance. Pour obtenir la description de ces voyants, consultez les guides sur le matériel, tel que le *Guide d'installation et de maintenance des appliances Cisco x90 Series Content Security Appliance*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Les spécifications de votre appliance, telles que les plages de températures, sont également indiquées dans ces documents.

Alerte : Délai d'expiration du réapprentissage de la batterie (événement RAID) sur le matériel 380 ou 680

Cette alerte peut indiquer un problème ou non. L'expiration du délai de réapprentissage de la batterie ne signifie pas en soi qu'il y a un problème au niveau du contrôleur RAID. Le contrôleur pourra récupérer lors du réapprentissage suivant. Veuillez surveiller votre courriel pour toute autre alerte RAID au cours des

prochaines 48 heures afin de vous assurer qu'il ne s'agit pas d'une répercussion d'un autre problème. Si vous ne voyez aucune autre alerte de type RAID émanant du système, vous pouvez l'ignorer en toute sécurité.

Problèmes relatifs au protocole HTTPS/au déchiffrement/aux certificats

Accès aux sites HTTPS à l'aide de politiques de routage avec critères de catégorie d'URL

Pour les requêtes HTTPS redirigées de manière transparente, le proxy Web doit communiquer avec le serveur de destination pour déterminer le nom du serveur et donc la catégorie d'URL dans laquelle il appartient. Pour cette raison, lorsque le proxy Web évalue l'appartenance au groupe de politiques de routage, il ne peut pas encore connaître la catégorie d'URL d'une requête HTTPS, car il n'a pas encore contacté le serveur de destination. Si le proxy Web ne connaît pas la catégorie d'URL, il ne peut pas faire correspondre la demande HTTPS transparente à une politique de routage définie par l'utilisateur, car les informations sont insuffisantes.

Par conséquent, les transactions HTTPS redirigées de manière transparente ne correspondent aux politiques de routage que si aucun groupe de politiques de routage et aucun profil d'identification n'a de critères d'appartenance. Si des politiques de routage ou des profils d'identification définis par l'utilisateur définissent ses membres par catégorie d'URL, les transactions HTTPS transparentes correspondent au groupe de politiques de routage par défaut.

Échecs de demandes HTTPS

HTTPS avec substituts basés sur IP et demandes transparentes

Si la requête HTTPS provient d'un client qui ne dispose pas des informations d'authentification d'une requête HTTP antérieure, AsyncOS échoue la requête HTTPS ou décrypte la requête HTTPS afin d'authentifier l'utilisateur, selon la façon dont vous configurez le proxy HTTPS. Utilisez le paramètre de demande transparente HTTPS sur la page Security Services > HTTPS Proxy (Services de sécurité > Proxy HTTPS) pour définir ce comportement. Consultez la section d'activation du proxy HTTPS dans la rubrique Politiques de déchiffrement.

Comportement différent du client « Hello » pour les catégories personnalisées et par défaut

Lors de l'analyse des captures de paquets, vous remarquerez peut-être que la liaison « Client Hello » est envoyée à des moments différents pour les politiques de transmission directe avec déchiffrement HTTPS de catégorie personnalisée et de catégorie (Web) par défaut.

Pour une page HTTPS transmise par la catégorie par défaut, la liaison Client Hello est envoyée avant la réception d'une liaison Client Hello du demandeur, et la connexion échoue. Pour une page HTTPS transmise par une catégorie d'URL personnalisée, le client Hello est envoyé après sa réception du client du demandeur et la connexion réussie.

Comme solution, vous pouvez créer une catégorie d'URL personnalisée avec une action directe pour les pages Web compatibles avec SSL 3.0 uniquement.

Contournement du déchiffrement pour des sites Web particuliers

Certains serveurs HTTPS ne fonctionnent pas comme prévu lorsque le trafic vers eux est déchiffré par un serveur proxy, comme le proxy Web. Par exemple, certains sites Web et leurs applications Web et applets associés, tels que les sites bancaires haute sécurité, gèrent une liste codée en dur de certificats approuvés au lieu de dépendre du magasin de certificats du système d'exploitation.

Vous pouvez contourner le déchiffrement pour le trafic HTTPS vers ces serveurs afin de vous assurer que tous les utilisateurs peuvent accéder à ces types de sites.

Étape 1 Créez une catégorie d'URL personnalisée qui contient les serveurs HTTPS concernés en configurant les propriétés avancées.

Étape 2 Créez une politique de déchiffrement qui utilise la catégorie d'URL personnalisée créée à l'étape 1 dans le cadre de son appartenance et définissez l'action pour la catégorie d'URL personnalisée sur Pass Through (Intercommunication).

Conditions et restrictions des exceptions au blocage pour le contenu intégré et le contenu mentionné

Les exceptions basées sur le référent sont prises en charge uniquement dans les politiques d'accès. Pour utiliser cette fonctionnalité avec le trafic HTTPS, avant de définir des exceptions dans les politiques d'accès, vous devez configurer le déchiffrement HTTPS des catégories d'URL que vous sélectionnerez pour les exceptions. Cette fonctionnalité ne sera opérante dans certaines conditions :

Note Lorsque des plages de temps sont configurées, elles reçoivent la priorité la plus élevée. L'indicateur de référence ne fonctionnera pas si le quota de plage de temps a été atteint.

- Si la connexion passe par un tunnel et que le déchiffrement HTTPS n'est pas activé, cette fonctionnalité ne fonctionnera pas pour les demandes envoyées aux sites HTTPS.
- Selon la RFC 2616, un client de navigateur pourrait avoir un interrupteur à bascule pour la navigation ouverte ou anonyme, qui activerait ou désactiverait respectivement l'envoi d'informations de provenance et de provenance. La fonctionnalité dépend exclusivement de l'en-tête du référent, et la désactivation de leur envoi empêcherait notre fonctionnalité de fonctionner.

- Selon la RFC 2616, les clients ne doivent pas inclure de champ d'en-tête referer dans une requête HTTP (non sécurisée) si la page de référence a été transférée avec un protocole sécurisé. Ainsi, toute requête d'un site basé sur HTTPS vers un site basé sur HTTP n'aura pas l'en-tête referer, ce qui fait que cette fonctionnalité ne fonctionne pas comme prévu.
- Lorsqu'une politique de déchiffrement est configurée de sorte qu'une catégorie personnalisée correspond à la politique de déchiffrement et que l'action est réglée sur Drop (Abandon), toute demande entrante pour cette catégorie sera abandonnée et aucun contournement ne sera effectué.

Alerte : Problème lié au certificat de sécurité

En règle générale, les informations sur le certificat racine que vous générez ou chargez dans l'appliance ne sont pas répertoriées comme autorité de certification racine approuvée dans les applications clientes. Par défaut, dans la plupart des navigateurs Web, lorsque les utilisateurs envoient des demandes HTTPS, un message d'avertissement de l'application cliente leur signale qu'il existe un problème avec le certificat de sécurité du site Web. Habituellement, le message d'erreur indique que le certificat de sécurité du site Web n'a pas été émis par une autorité de certification approuvée ou que le site Web a été certifié par une autorité inconnue. Certaines autres applications client ne présentent pas ce message d'avertissement aux utilisateurs et ne permettent pas aux utilisateurs d'accepter le certificat non reconnu.

Note **Navigateurs Mozilla Firefox :** le certificat que vous chargez doit contenir « basicConstraints=CA:TRUE » pour fonctionner avec les navigateurs Mozilla Firefox. Cette contrainte permet à Firefox de reconnaître le certificat racine comme une autorité racine approuvée.

Problèmes liés au service Cisco de vérification des identités

Outils de résolution des problèmes relatifs au service Cisco de vérification des identités

Les éléments suivants peuvent être utiles lors du dépannage de problèmes liés à Cisco ISE :

- L'utilitaire de test ISE, utilisé pour tester la connexion au serveur ISE, fournit des informations précieuses concernant la connexion. Il s'agit de l'option de **démarrage du test** sur la page Identity Services Engine; voir Se connecter aux services ISE/ISE-PIC, on page 180.
- Journaux ISE et proxy; voir Superviser l'activité du système au moyen de journaux, on page 483
- Commandes de CLI liées à ISE `iseconfig` et `isedata`, en particulier `isedata` pour confirmer le téléchargement de la balise SGT. Voir Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671 pour de plus amples informations.
- Les fonctions de suivi Web et de suivi des politiques peuvent être utilisées pour déboguer les problèmes de correspondance de politiques; par exemple, un utilisateur qui devrait être autorisé est bloqué, et

inversement. Voir Outil de résolution de problèmes liés aux politiques : Suivi des politiques, on page 653 pour de plus amples informations.

- Capture de paquets, on page 661 si Collaboration avec le service d'assistance , on page 663.
- Pour vérifier l'état des certificats, vous pouvez utiliser l'utilitaire openssl (ocsp), disponible à partir de https://www.openssl.org/ .

Problèmes de connexion au serveur ISE

Problèmes de certificats

Les serveurs Secure Web Appliance et ISE utilisent des certificats pour s'authentifier mutuellement et assurer le succès de la connexion. Ainsi, chaque certificat présenté par une entité devrait être reconnaissable par une autre. Par exemple, si le certificat client de Secure Web Appliance est autosigné, le même certificat doit être présent dans la liste des certificats approuvés sur le ou les serveurs ISE appropriés. De même, si le certificat client de l'appliance Web est signé par une autorité de certification, le certificat racine de l'autorité de certification doit être présent sur le ou les serveurs ISE appropriés. Des exigences similaires s'appliquent aux certificats Admin et pxGrid liés au serveur ISE.

Les exigences du certificat et l'installation sont décrites dans Survol du moteur du service de vérification des identités Identity Services Engine (ISE) et du service du connecteur d'identité passive ISE (ISE-PIC), on page 173. Si vous rencontrez des problèmes liés aux certificats, vérifiez les éléments suivants :

- Si vous utilisez des certificats signés par une autorité de certification :
  - Vérifiez que l'autorité de certification racine qui signe les certificats Admin et pxGrid est présente dans Secure Web Appliance.
  - Vérifiez que le certificat de signature de l'autorité de certification racine pour le certificat client de l'appliance Web se trouve dans la liste des certificats approuvés sur le serveur ISE.
- Si vous utilisez des certificats autosignés :
  - Vérifiez que le certificat client d'appliance Web, généré sur le Secure Web Appliance et téléchargé, a été chargé sur le serveur ISE et qu'il est présent dans la liste des certificats approuvés des serveurs ISE.
  - Vérifiez que les certificats ISE Admin et pxGrid (générés sur le serveur ISE et téléchargés) ont été téléchargés dans Secure Web Appliance et sont présents dans la liste de certificats ISE correspondante.
- Certificats expirés :
  - Confirmez que les certificats valides au moment du téléchargement n'ont pas expiré.

Résultats du journal indiquant un problème de certificat

Le fragment de code du journal de service ISE suivant montre un délai de connexion client en raison d'un certificat manquant ou non valide.

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

Ces entrées de journal de niveau trace sur le Secure Web Appliance montrent qu'après 30 secondes, les tentatives de connexion au serveur ISE sont terminées.

Problèmes de réseau

Si la connexion au serveur ISE échoue pendant le test de démarrage sur la page du moteur de services de vérification des identités (Se connecter aux services ISE/ISE-PIC, on page 180), vérifiez la connectivité au serveur ISE configuré sur les ports 443 et 5222.

Le port 5222 est le port officiel du protocole XMPP (Extensible Messaging and Presence Protocol) client-serveur et est utilisé pour la connexion au serveur ISE. il est également utilisé par des applications telles que Jabber et Google Talk. Notez que certains pare-feu sont configurés pour bloquer le port 5222.

Les outils qui peuvent être utilisés pour vérifier la connectivité comprennent `tcpdump`

Autres problèmes de connectivité du serveur du service Cisco de vérification des identités

Les problèmes suivants peuvent provoquer un échec lorsque Secure Web Appliance tente de se connecter au serveur ISE :

- Les licences sur le serveur ISE ont expiré.
- L'état du nœud pxGrid est « non connecté » sur la page Administration > pxGrid Services (Administration > Services pxGrid) du serveur ISE. Assurez-vous que l'option Enable Auto-Registration (activer l'enregistrement automatique) est sélectionnée sur cette page.
- Des clients Secure Web Appliance obsolètes (en particulier « test_client » ou « pxgrid_client ») sont présents sur le serveur ISE. Ceux-ci doivent être supprimés; voir Administration > pxGrid Services > Clients (Administration > Services pxGrid > Clients) sur le serveur ISE.

- Secure Web Appliance tente de se connecter au serveur ISE avant que tous ses services soient opérationnels.

  Certaines modifications sur le serveur ISE, telles que les mises à jour de certificats, nécessitent le redémarrage du serveur ISE ou des services qui y sont exécutés. Toute tentative de connexion au serveur ISE pendant ce délai échouera; cependant, la connexion finit par réussir.

Messages du journal critiques liés au service Cisco de vérification des identités

Cette section contient des explications concernant les messages de journalisation critiques liés à ISE sur les Secure Web Appliance :

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out` (En attente de la connexion du client expiré)

  Le processus ISE de Secure Web Appliancen'a pas réussi à se connecter au serveur ISE pendant 30 secondes.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing. (Certificat ou clé du client WSA manquant) Veuillez vérifier la configuration ISE`

  Le certificat client de l'appliance Web et la clé n'ont pas été téléchargés ou générés sur la page de configuration du moteur Identity Services Engine de Secure Web Appliance.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server` (le service ISE a dépassé la durée de déconnexion maximale autorisée avec le serveur ISE)

  Le processus ISE de Secure Web Appliancen'a pas pu se connecter au serveur ISE pendant 120 secondes et s'est arrêté.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed ...` (Échec de l'abonnement aux mises à jour)

  Le processus ISE de Secure Web Appliance n'a pas pu s'abonner au serveur ISE pour les mises à jour.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: ...`(Impossible de créer le client ISE)

  Erreur interne lors de la création du client ISE de Secure Web Appliancepour la connexion du serveur ISE.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: ...` (Échec du téléchargement en bloc)

  Erreur interne indiquant l'échec du téléchargement en bloc des groupes SGT lors de la connexion ou de la reconnexion.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service. Error: ...` (Impossible de démarrer le service.)

  Le service ISE de Secure Web Appliance n'a pas pu démarrer.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal ...` (Impossible d'envoyer le signal de disponibilité)

  Le service ISE de Secure Web Appliance n'a pas pu envoyer de signal de disponibilité à Heimdall.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal ...` (Impossible d'envoyer le signal de redémarrage)

  Le service ISE de Secure Web Appliance n'a pas pu envoyer de signal de redémarrage à heimdall.

Problèmes liés aux catégories d'URL personnalisées et externes

Problèmes de téléchargement d'un fichier de flux en direct externe

Lors de la création et de la modification de catégories d'URL personnalisées et externes et de la fourniture d'un fichier de **flux en direct externe** (au **format de flux Cisco** ou au **format de flux Office 365**), vous devez cliquer sur le bouton **Get File** (Obtenir le fichier) pour établir la connexion au serveur indiqué, ainsi que pour télécharger et analyser le fichier. La progression et les résultats de ce processus sont affichés; si des erreurs se produisent, elles sont décrites. Corrigez les problèmes et réessayez de télécharger le fichier.

Il existe quatre types d'erreurs possibles :

- Exceptions de connexion

  `Failed to resolve server hostname` (Échec de la résolution du nom d'hôte du serveur) : l'URL fournie comme emplacement du fichier de flux n'est pas valide; indiquez une URL correcte pour résoudre ce problème.

- Erreurs de protocole

  `Authentication failed due to invalid credentials` (Échec de l'authentification en raison d'informations d'authentification non valides) : échec de l'authentification du serveur; indiquez le nom d'utilisateur et la phrase secrète corrects pour la connexion au serveur.

  `The requested file is not found on the server` (Le fichier demandé est introuvable sur le serveur) : l'URL fournie pour le fichier de flux pointe vers une ressource non valide. Assurez-vous que le bon fichier est disponible sur le serveur précisé.

- Erreurs de validation de contenu

  `Failed to validate the content of the field` (Échec de la validation du contenu du champ) : le contenu du fichier de flux n'est pas valide.

- Erreurs d'analyse

  - Le fichier au format de flux Cisco .csv doit contenir une ou plusieurs entrées, où chaque entrée est une adresse de site ou une chaîne d'expression régulière valide, suivie d'une virgule, puis du type d'adresse (qui peut être un `site` ou une `expression régulière`). Si cette convention n'est pas suivie pour une entrée du fichier de flux, une erreur d'analyse est renvoyée.

    De plus, n'incluez pas `http://` ou `https://` dans une entrée `site` dans le fichier, sous peine d'entraîner une erreur. En d'autres termes, `www.exemple.com` est analysé correctement, tandis que `http://www.exemple.com` produit une erreur.

- Le fichier de flux XML obtenu à partir d'un serveur Microsoft est analysé par un analyseur syntaxique XML standard. Toute incohérence dans les balises XML est également signalée comme des erreurs d'analyse.

Le numéro de ligne d'une erreur d'analyse est inclus dans le journal. Par exemple :

`Line 8: 'www.anyurl.com' - Line is missing address or address-type field` (Ligne 8 : « www.anyurl.com » : champ d'adresse ou de type d'adresse manquant sur la ligne). La ligne 8 du fichier de flux ne contient pas d'adresse ou de modèle d'expression régulière, ni de type d'adresse.

`Line 12: 'www.test.com' - Unknown address type.` (Ligne 12 : « www.test.com » – Type d'adresse inconnu). La ligne 12 a un type d'adresse non valide; la valeur addresstype peut être `site` ou `regex`.

Problème de type MIME sur le serveur IIS pour les fichiers .CSV

Lorsque vous fournissez un fichier .csv pour l'option **External Live Feed Category** > **Cisco Feed Format** (Catégorie de flux en direct externe > Format de flux Cisco) lors de la création et de la modification de catégories d'URL personnalisées et externes, vous pouvez rencontrer l'erreur « 406 not acceptable » lors de la récupération du fichier si le serveur de format de flux Cisco utilise le logiciel Internet Information Services (IIS) version 7 ou 8. De même, le journal `feedsd` renverra un résultat comme : `31 May 2016 16:47:22 (GMT +0200) Warning: Protocol Error: 'HTTP error while fetching file from the server'` (31 mai 2016 16:47:22 (GMT +0200) Avertissement : Erreur de protocole : « Erreur HTTP lors de la récupération du fichier sur le serveur »).

En effet, le type MIME par défaut pour les fichiers .csv sur IIS est `application/csv` plutôt que `text/csv`. Vous pouvez résoudre le problème en vous connectant au serveur IIS et en modifiant l'entrée MIME type pour les fichiers .csv afin qu'elle corresponde à la valeur `text/csv`.

Fichier de flux mal formé après un copier-coller

Si vous copiez et collez le contenu d'un fichier de flux .csv (texte) d'un système UNIX ou OS X vers un système Windows, un retour à la ligne supplémentaire (`\r`) est ajouté automatiquement, ce qui peut rendre le fichier de flux mal formé.

Si vous créez manuellement le fichier .csv ou si vous transférez le fichier d'un système UNIX ou OS X vers un serveur Windows à l'aide de SCP, FTP ou POST, il ne devrait y avoir aucun problème.

Problèmes de journalisation

Catégories d'URL personnalisées n'apparaissant pas dans les entrées du journal d'accès

Lorsqu'un groupe de politiques d'accès Web a une catégorie d'URL personnalisée définie sur Monitor (Superviser) et qu'un autre composant, comme les filtres de réputation Web ou le moteur DVS, prend la

décision finale d'autoriser ou de bloquer une demande d'URL dans la catégorie d'URL personnalisée, l'entrée du journal d'accès pour la demande affiche la catégorie d'URL prédéfinie au lieu de la catégorie d'URL personnalisée.

Journalisation des transactions HTTPS

Les transactions HTTPS dans les journaux d'accès semblent similaires aux transactions HTTP, mais avec des caractéristiques légèrement différentes. Les informations qui sont enregistrées dépendent de si la transaction a été explicitement envoyée ou redirigée de manière transparente vers le proxy HTTPS :

- **TUNNEL.** Cela est écrit dans le journal des accès lorsque la demande HTTPS est redirigée de manière transparente vers le proxy HTTPS.
- **CONNECT.** Cela est écrit dans le journal des accès lorsque la demande HTTPS a été explicitement envoyée au proxy HTTPS.

Lorsque le trafic HTTPS est déchiffré, les journaux d'accès contiennent deux entrées pour une transaction :

- TUNNEL ou CONNECT selon le type de demande traitée.
- La méthode HTTP et l'URL déchiffrée. Par exemple, « GET https://ftp.exemple.com ».

L'URL complète n'est visible que lorsque le proxy HTTPS déchiffre le trafic.

Alerte : impossible de maintenir le débit des données générées

AsyncOS pour le Web envoie un e-mail critique aux destinataires des alertes configurés lorsque le processus de journalisation interne abandonne les événements de transaction Web en raison d'une mémoire tampon pleine.

Par défaut, lorsque le proxy Web subit une charge très élevée, le processus de journalisation interne met en mémoire tampon les événements pour les enregistrer plus tard, lorsque la charge du proxy Web diminue. Quand la mémoire tampon de journalisation est complètement pleine, le proxy Web continue de traiter le trafic, mais le processus de journalisation n'enregistre pas certains événements dans les journaux d'accès ou dans le rapport de suivi Web. Cela peut se produire lors d'un pic du trafic Web.

Cependant, une mémoire tampon de journalisation pleine peut également se produire lorsque l'appliance est en dépassement de capacité pendant une période prolongée. AsyncOS pour le Web continue d'envoyer des e-mails critiques toutes les quelques minutes jusqu'à ce que le processus de journalisation ne supprime plus de données.

Le message critique contient le texte suivant :

`Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.` (Client de rapports : Le système de rapports n'est pas en mesure de maintenir le débit des données générées. Toutes les nouvelles données générées seront perdues.)

Si AsyncOS pour le Web envoie ce message critique de manière continue ou fréquente, l'appliance est peut-être en surcapacité. Communiquez avec l'assistance client de Cisco pour vérifier si vous avez besoin d'une capacité Secure Web Appliance supplémentaire.

Problème d'utilisation de l'outil tiers Log-Analyzer avec les journaux d'accès W3C

Si vous souhaitez utiliser un analyseur de journaux tiers pour lire et analyser les journaux d'accès W3C, vous devrez peut-être inclure le champ « timestamp » (horodatage). Le champ timestamp (horodatage) de W3C affiche l'heure depuis l'époque UNIX et la plupart des analyseurs de journaux ne comprennent l'heure que dans ce format.

Problèmes de politique

- Politique d'accès non configurable pour HTTPS, on page 651
- Problèmes d'objets bloqués, on page 637
- Disparition du profil d'identification de la politique, on page 652
- Échecs de correspondance de politiques, on page 652
- Outil de résolution de problèmes liés aux politiques : Suivi des politiques, on page 653
- Voir également : Accès aux sites HTTPS à l'aide de politiques de routage avec critères de catégorie d'URL, on page 642

Politique d'accès non configurable pour HTTPS

Lorsque le proxy HTTPS est activé, les politiques de déchiffrement prennent en charge toutes les décisions relatives aux politiques HTTPS. Vous ne pouvez plus définir l'appartenance à un groupe de politiques d'accès et de routage par HTTPS, et vous ne pouvez plus configurer les politiques d'accès pour bloquer les transactions HTTPS.

Si certaines appartenances à des groupes de politiques d'accès et de routage sont définies par HTTPS et si certaines politiques d'accès bloquent HTTPS, lorsque vous activez le proxy HTTPS, ces groupes de politiques d'accès et de routage sont désactivés. Vous pouvez choisir d'activer les politiques à tout moment, mais toutes les configurations liées à HTTPS sont supprimées.

Problèmes d'objets bloqués

- Certains fichiers Microsoft Office ne sont pas bloqués, on page 637
- Le blocage des types d'objets exécutables DOS bloque les mises à jour pour Windows OneCare, on page 637

Certains fichiers Microsoft Office ne sont pas bloqués

Lorsque vous bloquez des fichiers Microsoft Office dans la section Block Object Type (Bloquer le type d'objet), il est possible que certains fichiers Microsoft Office ne soient pas bloqués.

Si vous devez bloquer tous les fichiers Microsoft Office, ajoutez **application/x-ole** dans le champ Block Personal MIME Types (Bloquer les types MIME personnalisés). Cependant, le blocage de ce type MIME personnalisé bloque également tous les types de formats d'objets composés Microsoft, tels que les fichiers Visio et certaines applications tierces.

Le blocage des types d'objets exécutables DOS bloque les mises à jour pour Windows OneCare

Lorsque vous configurez Secure Web Appliance pour bloquer les types d'objets exécutables DOS, l'appliance bloque également les mises à jour pour Windows OneCare.

Disparition du profil d'identification de la politique

La désactivation d'un profil d'identification supprime ce dernier des politiques associées. Vérifiez que le profil d'identification est activé, puis ajoutez-le à nouveau à la politique.

Échecs de correspondance de politiques

La politique n'est jamais appliquée

Si plusieurs profils d'identification ont des critères identiques, AsyncOS affecte les transactions au premier profil d'identification qui correspond. Par conséquent, les transactions ne correspondent jamais aux profils d'identification identiques supplémentaires, et toutes les politiques qui s'appliquent à ces profils d'identification identiques ultérieurs ne sont jamais mises en correspondance ou appliquées.

Les demandes HTTPS et FTP via HTTP correspondent uniquement aux politiques d'accès qui ne nécessitent pas d'authentification

Configurez l'appliance pour utiliser les adresses IP comme substitution lorsque le chiffrement des informations d'identification est activé.

Lorsque le chiffrement des informations d'authentification est activé et configuré pour utiliser des témoins comme type de substitution, l'authentification ne fonctionne pas avec les requêtes HTTPS ou FTP sur HTTP. En effet, le proxy Web redirige les clients vers le proxy Web lui-même pour l'authentification à l'aide d'une connexion HTTPS si le chiffrement des informations d'authentification est activé. Une fois l'authentification réussie, le proxy Web redirige les clients vers le site Web d'origine. Afin de continuer à identifier l'utilisateur, le proxy Web doit utiliser un moyen de substitution (l'adresse IP ou un témoin). Cependant, l'utilisation d'un témoin pour suivre les utilisateurs entraîne le comportement suivant si les demandes utilisent HTTPS ou FTP sur HTTP :

- **HTTPS.** Le proxy Web doit résoudre l'identité de l'utilisateur avant d'affecter une politique de déchiffrement (et, par conséquent, de déchiffrer la transaction), mais il ne peut pas obtenir de témoin pour identifier l'utilisateur à moins de déchiffrer la transaction.
- **FTP sur HTTP.** Le dilemme lié à l'accès aux serveurs FTP à l'aide de FTP sur HTTP est le même que celui de l'accès à des sites HTTPS. Le proxy Web doit résoudre l'identité de l'utilisateur avant d'affecter une politique d'accès, mais il ne peut pas définir le témoin de la transaction FTP.

Par conséquent, les requêtes HTTPS et FTP sur HTTP correspondent uniquement aux politiques d'accès qui ne nécessitent pas d'authentification. En règle générale, elles correspondent à la politique d'accès globale, car elle ne nécessite jamais d'authentification.

Politique globale de correspondances des utilisateurs pour les demandes HTTPS et FTP via HTTP

Lorsque l'appliance utilise l'authentification basée sur les témoins, le proxy Web n'obtient pas les informations sur les témoins des clients pour les demandes HTTPS et FTP sur HTTP. Par conséquent, elle ne peut pas obtenir le nom d'utilisateur à partir du témoin.

Les demandes HTTPS et FTP sur HTTP correspondent toujours au profil d'identification en fonction des autres critères d'appartenance, mais le proxy Web n'invite pas les clients à s'authentifier, même si le profil d'identification l'exige. Au lieu de cela, le proxy Web définit le nom d'utilisateur sur NULL et considère l'utilisateur comme non authentifié.

Ensuite, lorsque la demande non authentifiée est évaluée par rapport à une politique, elle ne correspond qu'à une politique qui spécifie « Toutes les identités » et s'applique à « Tous les utilisateurs ». En règle générale, il s'agit de la politique globale, par exemple la politique d'accès globale.

Politique d'accès incorrecte attribuée à l'utilisateur

- Les clients de votre réseau utilisent l'indicateur d'état de connectivité de réseau (NCSI)
- Secure Web Appliance utilise l'authentification NTLMSSP.
- Le profil d'identification utilise des substitutions basées sur IP

Un utilisateur peut être identifié à l'aide des informations d'authentification de l'ordinateur au lieu de ses propres informations d'authentification et, par conséquent, être affecté à une politique d'accès incorrecte.

Solution :

Réduisez la valeur du délai d'expiration de substitution pour les informations d'authentification de l'ordinateur.

Étape 1 Utilisez la commande d'interface de ligne de commande `advancedproxyconfig > authentication`.

Étape 2 Saisissez le délai d'expiration de substitution pour les informations d'authentification de l'ordinateur.

Incompatibilité de suivi des politiques après la modification des paramètres de politique

Lorsque vous modifiez des paramètres tels que la politique d'accès, des profils d'identification et d'utilisateurs, sélectionnez un ou plusieurs profils d'identification ou une sélection de groupes et d'utilisateurs, les modifications prennent quelques minutes avant d'être appliquées.

Outil de résolution de problèmes liés aux politiques : Suivi des politiques

À propos de l'outil de suivi des politiques

L'outil de suivi des politiques peut émuler une demande d'un client, puis détailler comment le proxy Web traite cette demande. Il peut être utilisé pour suivre les demandes des clients et déboguer le traitement des politiques lors du dépannage de problèmes de proxy Web. Vous pouvez effectuer un suivi de base ou saisir des paramètres de suivi avancés et remplacer les options.

Note Lorsque vous utilisez l'outil de suivi des politiques, le proxy Web n'enregistre pas les demandes dans le journal des accès ou dans la base de données de rapports.

L'outil de suivi des politiques évalue les demandes en fonction des politiques utilisées par le proxy Web uniquement. Il s'agit des politiques d'accès, de gestion HTTPS chiffré, de routage, de sécurité des données et d'analyse des programmes malveillants sortants.

Note Les politiques SOCKS et DLP externes ne sont pas évaluées par l'outil de suivi des politiques.

Suivi des demandes des clients

Note Vous pouvez utiliser la commande `maxhttpheadersize` de l'interface de ligne de commande pour modifier la taille maximale de l'en-tête HTTP des demandes de proxy. L'augmentation de cette valeur peut atténuer les échecs du suivi des politiques qui peuvent se produire lorsque l'utilisateur spécifié appartient à un grand nombre de groupes d'authentification ou lorsque la taille de l'en-tête de réponse est supérieure à la taille maximale actuelle. Consultez Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671 pour plus d'informations sur cette commande.

Étape 1 Choisissez **System Administration > Policy Trace** (Administration système > Suivi de politique).

Étape 2 Entrez l'URL dont vous voulez effectuer le suivi dans le champ Destination URL (URL de destination).

Étape 3 (Facultatif) Saisissez d'autres paramètres d'émulation :

Pour émuler...	Saisissez...
L'adresse IP source du client utilisée pour effectuer la demande.	Une adresse IP dans le champ Client IP Address (Adresse IP du client). **Note** Si une adresse IP n'est pas spécifiée, AsyncOS utilise localhost. En outre, les SGT (balises de groupe de sécurité) ne peuvent pas être extraites et les politiques basées sur les SGT ne seront pas mises en correspondance.

Pour émuler...	Saisissez...
Les informations d'authentification et d'identification utilisées pour effectuer la demande.	Saisissez le nom d'utilisateur dans le champ User Name (Nom d'utilisateur), puis choisissez Identity Services Engine (Moteur de services de vérification des identités) ou un domaine d'authentification dans la liste déroulante Authentication/Identification (Authentification/Identification). **Note** Seules les options activées sont disponibles. En d'autres termes, les options d'authentification et l'option ISE ne sont disponibles que si elles sont toutes deux activées. Pour l'authentification de l'utilisateur que vous entrez ici, l'utilisateur doit déjà s'être authentifié avec succès à l'aide de la commande Secure Web Appliance.

Étape 4 Cliquez sur **Find Policy** (Rechercher une politique).

Le résultat du suivi de politique s'affiche dans le volet Results (Résultats).

Note Pour une transaction d'intercommunication HTTPS, l'outil de suivi des politiques contourne l'analyse supplémentaire et aucune politique d'accès n'est associée à la transaction. De même, pour une transaction de déchiffrement HTTPS, l'outil ne peut pas déchiffrer la transaction pour déterminer la politique d'accès appliquée. Dans les deux cas, ainsi que pour les transactions d'abandon, les résultats du suivi affichent : « Access Policy: Not Applicable » (Politique d'accès : sans objet).

Note Si l'adresse IP du client indiquée n'est pas routable, les résultats du suivi affichent ce qui suit : « Connection Trace: Connection to Origin Server: Failed » (Suivi de connexion : Connexion au serveur d'origine : échec).

What to do next

Thèmes connexes

- Avancé : Détails de la demande, on page 655
- Avancé : Remplacements des détails des réponses, on page 656

Avancé : Détails de la demande

Vous pouvez utiliser les paramètres du volet Request Details (Détails de la demande) de la page Policy Trace (Suivi de politique), section Advanced (Avancé), afin de régler la demande d'analyse des programmes malveillants sortants pour ce suivi de politique.

Étape 1 Développez la section **Advanced** (Avancé) de la page Policy Trace (Suivi de politique).

Étape 2 Renseignez les champs du volet Request Details (Détails de la demande) selon vos besoins :

Paramètres	Description
Proxy Port (Port du serveur proxy)	Sélectionnez un port proxy spécifique à utiliser pour la demande de suivi afin de tester l'appartenance à la politique en fonction du port proxy.
User Agent (Agent d'utilisateur)	Indiquez l'agent utilisateur à simuler dans la demande.

Paramètres	Description
Time of Request (Heure de la demande)	Indiquez la date et l'heure à simuler dans la demande.
Upload File (Téléverser le fichier)	Choisissez un fichier local pour simuler le chargement dans la demande. Lorsque vous spécifiez un fichier à télécharger ici, le proxy Web simule une requête HTTP POST au lieu d'une demande GET.
Object Size (Taille de l'objet)	Saisissez la taille de l'objet de la demande en octets. Vous pouvez entrer K, M ou G pour représenter les kilooctets, les mégaoctets ou les gigaoctets.
MIME Type (Type MIME)	Entrez le type MIME.
Anti-malware Scanning Verdicts (Verdicts de l'analyse de protection contre les programmes malveillants)	Pour remplacer un verdict d'analyse Webroot, McAfee ou Sophos, choisissez le type spécifique de verdicts à remplacer.

Étape 3 Cliquez sur **Find Policy** (Rechercher une politique).

Le résultat du suivi de politique s'affiche dans le volet Results (Résultats).

Avancé : Remplacements des détails des réponses

Vous pouvez utiliser les paramètres du volet Response Detail Overrides (Remplacement des détails des réponses) de la page Policy Trace (Suivi des politiques), section Advanced (Avancé), pour « altérer » certains aspects de la réponse aux politiques d'accès Web dans le cadre de ce suivi.

Étape 1 Développez la section **Advanced** (Avancé) de la page Policy Trace (Suivi de politique).

Étape 2 Renseignez les champs du volet Response Detail Overrides (Remplacer les détails des réponses), au besoin :

Paramètres	Description
URL Category (Catégorie URL)	Utilisez ce paramètre pour remplacer la catégorie de transaction d'URL de la réponse de suivi. Choisissez une catégorie qui doit remplacer la catégorie d'URL dans les résultats des réponses.
Application	De même, utilisez ce paramètre pour remplacer la catégorie d'application de la réponse de suivi. Choisissez une catégorie qui doit remplacer la catégorie d'application dans les résultats des réponses.
Object Size (Taille de l'objet)	Entrez la taille de l'objet de réponse en octets. Vous pouvez entrer K, M ou G pour représenter les kilooctets, les mégaoctets ou les gigaoctets.
MIME Type (Type MIME)	Entrez un type MIME.

Paramètres	Description
Web Reputation Score (Score de réputation Web)	Saisissez un score de réputation Web compris entre -10.0 et 10.0. Un score de réputation Web égal à -100 signifie une « absence de score ».
Anti-malware Scanning Verdicts (Verdicts de l'analyse de protection contre les programmes malveillants)	Utilisez ces options pour remplacer des verdicts d'analyse spécifiques de protection contre les programmes malveillants fournis dans la réponse de suivi. Choisissez les verdicts qui doivent remplacer les verdicts de contrôle Webroot, McAfee et Sophos dans les résultats de réponse.

Étape 3 Cliquez sur **Find Policy** (Rechercher une politique).

Le résultat du suivi de politique s'affiche dans le volet Results (Résultats).

Problèmes de réputation et d'analyse des fichiers

Voir la section Résolution des problèmes liés à la réputation et à l'analyse des fichiers , on page 344.

Problèmes de redémarrage

L'appliance virtuelle fonctionnant sur KVM se bloque au redémarrage

Note Il s'agit d'un problème KVM qui peut changer à tout moment.

Pour plus d'informations, consultez https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html and https://bugs.launchpad.net/qemu/+bug/1329956.

Étape 1 Vérifiez les éléments suivants :

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

Étape 2 Si la valeur ci-dessus est définie sur Y :

a) Arrêtez vos appliances virtuelles et réinstallez le module de noyau KVM :

```
rmmod kvm_intel  modprobe kvm_intel enable_apicv=N
```

b) Redémarrez votre appliance virtuelle.

Appliances matérielles : réinitialisation à distance de l'alimentation des appliances

Before you begin

- Obtenez et configurez un utilitaire qui peut gérer les périphériques à l'aide d'IPMI version 2.0.
- Apprenez à utiliser les commandes IPMI prises en charge. Consultez la documentation de votre outil IPMI.

Si une appliance matérielle nécessite une réinitialisation matérielle, vous pouvez redémarrer le châssis de l'appliance à distance à l'aide d'un outil IPMI (Intelligent Platform Management Interface) tiers.

Restrictions

- Le redémarrage à distance est disponible uniquement sur certains matériels. Pour en savoir plus, consultez Activation du redémarrage à distance , on page 579.
- Si vous souhaitez pouvoir utiliser cette fonctionnalité, vous devez l'activer avant de devoir l'utiliser. Pour de plus amples renseignements, consultez la section Activation du redémarrage à distance , on page 579.
- Seules les commandes IPMI suivantes sont prises en charge : status, on, off, cycle, reset, diag, soft. L'exécution de commandes non prises en charge produira une erreur de type « privilèges insuffisants ».

Étape 1 Utilisez IPMI pour émettre une commande de redémarrage prise en charge à l'adresse IP attribuée au port de redémarrage à distance, que vous avez configuré plus tôt, avec les informations d'authentification requises.

Par exemple, à partir d'une machine de type UNIX prenant en charge IPMI, vous pourriez exécuter la commande :

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

Pour les modèles S195, S395 et S695, utilisez :

```
ipmitool -I lanplus -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

où `192.0.2.1` est l'adresse IP attribuée au port de redémarrage à distance et remoteresetuser et la phrase secrète sont les informations d'authentification que vous avez saisies lors de l'activation de cette fonctionnalité.

Étape 2 Attendez au moins onze minutes que l'appliance redémarre.

Problèmes d'accès au site

Impossible d'accéder aux URL qui ne prennent pas en charge l'authentification

Il s'agit d'une liste partielle d'applications qui ne peuvent pas être utilisées lorsque Secure Web Appliance est déployé en mode transparent, car ils ne prennent pas en charge l'authentification.

- Mozilla Thunderbird

- Mises à jour d'Adobe Acrobat
- HttpBridge
- Subversion, par CollabNet
- Microsoft Windows Update
- Microsoft Visual Studio

Solution : Créez une classe d'utilisateurs pour l'URL qui ne nécessite pas d'authentification.

Thèmes connexes

- Contournement de l'authentification, on page 143

Impossible d'accéder aux sites avec les requêtes POST

Lorsque la première requête client de l'utilisateur est une requête POST et que l'utilisateur doit toujours s'authentifier, le corps de la requête est perdu. Cela peut poser un problème lorsque la requête POST concerne une application avec la fonctionnalité de connexion unique de contrôle d'accès utilisée.

Solutions :

- Demandez aux utilisateurs de s'authentifier d'abord auprès du proxy Web en demandant une autre URL dans le navigateur avant de se connecter à une URL qui utilise POST comme première demande.
- Contournez l'authentification pour les URL qui utilisent POST comme première requête.

Note Lorsque vous utilisez le contrôle d'accès, vous pouvez contourner l'authentification pour l'URL du service d'assertion aux consommateurs (ACS) configurée dans la politique d'authentification de l'application.

Thèmes connexes

- Contournement de l'authentification, on page 143.

Problèmes de proxy en amont

- Le proxy en amont ne reçoit pas les informations d'authentification de base, on page 659
- Échec des demandes du client au proxy en amont, on page 660

Le proxy en amont ne reçoit pas les informations d'authentification de base

Si l'appliance et le proxy en amont utilisent l'authentification avec NTLMSSP, selon les configurations, l'appliance et le proxy en amont peuvent s'engager dans une boucle infinie de demande d'informations d'authentification. Par exemple, si le proxy en amont nécessite une authentification de base, mais que l'appliance nécessite une authentification NTLMSSP, l'appliance ne pourra jamais transmettre avec succès les informations d'authentification de base au proxy en amont. Cela est dû aux limites des protocoles d'authentification.

Échec des demandes du client au proxy en amont

Configuration :

- Secure Web Appliance et le serveur proxy en amont utilise l'authentification de base.
- Le chiffrement des informations d'authentification est activé sur le Secure Web Appliance en aval.

Les demandes des clients échouent sur le proxy en amont, car le proxy Web reçoit un en-tête HTTP « Authorization » des clients, mais le serveur proxy en amont nécessite un en-tête HTTP « Proxy-Authorization ».

Unable to Route FTP Requests Via an Upstream Proxy (Impossible d'acheminer les requêtes FTP de la voie de routage par le biais d'un proxy en amont)

Si votre réseau contient un proxy en amont qui ne prend pas en charge les connexions FTP, vous devez créer une politique de routage qui s'applique à toutes les identités et uniquement aux demandes FTP. Configurez cette politique de routage pour accéder directement aux serveurs FTP ou à un groupe de proxy dont tous les proxys soutiennent les connexions FTP.

Appliances virtuelles

Ne pas utiliser les options de réinitialisation forcée, de mise hors tension ou de réinitialisation au démarrage d'AsyncOS

Les actions suivantes sur votre hôte virtuel équivalent au débranchement d'une appliance matérielle et ne sont pas prises en charge, en particulier au démarrage d'AsyncOS :

- Dans KVM, l'option Force Reset (Réinitialisation forcée).
- Dans VMWare, les options Power Off et Reset (Arrêt et réinitialisation). (Ces options peuvent être utilisées en toute sécurité une fois que l'appliance est complètement installée.)

La connectivité réseau sur les déploiements KVM fonctionne au départ, puis échoue

Problème

La connectivité réseau est perdue après avoir fonctionné précédemment.

Solution

Il s'agit d'un problème lié à KVM. Reportez-vous à la section « KVM : La connectivité réseau fonctionne initialement, puis échoue » dans la documentation d'OpenStack à l'adresse http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html

Ralentissement, problèmes de surveillance et utilisation intense du processeur sur les déploiements KVM

Problème

Les performances de l'appliance sont lentes, des problèmes de supervision se produisent et l'appliance affiche une utilisation du processeur inhabituellement élevée lors de l'exécution sur une machine virtuelle Ubuntu.

Solution

Installez les dernières mises à jour du système d'exploitation de l'hôte à partir d'Ubuntu.

Résolution de problèmes d'ordre général pour les appliances virtuelles fonctionnant sur des hôtes Linux

Problème

Les problèmes liés aux appliances virtuelles fonctionnant sur les déploiements KVM peuvent être liés à des problèmes de configuration du système d'exploitation de l'hôte.

Solution

Consultez la section de dépannage et d'autres informations dans le *Guide de déploiement et d'administration de la virtualisation*, disponible à l'adresse suivante :

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf.

Problèmes du WCCP

• Entrées de port maximales, on page 661

Entrées de port maximales

Dans les déploiements qui font appel à WCCP, le nombre maximal d'entrées de port est de 30 pour les ports HTTP, HTTPS et FTP combinés.

Capture de paquets

• Démarrage d'une capture de paquets, on page 662
• Gestion des fichiers de capture de paquets, on page 663

L'appliance permet de capturer et d'afficher les paquets TCP/IP et d'autres paquets transmis ou reçus sur le réseau auquel l'appliance est connectée.

Note La fonction de capture de paquets est similaire à la commande tcpdump d'Unix.

Secure Web Appliance ne prend pas en charge la capture de paquets pour les interfaces NIC appairées. La capture de paquets sera appliquée uniquement pour l'interface active. Par exemple, si P1 et P2 sont appairées, P1 et P2 ne seront pas configurées dans l'interface utilisateur ou l'interface de ligne de commande.

Démarrage d'une capture de paquets

Étape 1 Choisissez **Support and Help > Packet Capture** (Assistance et aide > Capture de paquets).

Étape 2 (Facultatif) Cliquez sur **Edit Settings** (Modifier les paramètres) pour modifier les paramètres de capture de paquets.

Option	Description
Limite de taille du fichier de capture	Spécifie la taille maximale que le fichier de capture peut atteindre. Une fois la limite atteinte, les données sont supprimées et un nouveau fichier démarre, sauf si le paramètre Capture Duration (Durée de capture) est renseigné par « Run Capture Until File Size Limit Reached » (Exécuter la capture jusqu'à la limite de taille du fichier atteint).
Capture Duration (Durée de la capture)	Options en cas d'arrêt automatique de la capture Choisissez parmi : • **Run Capture Until File Size Limit Reached** (Exécuter la capture jusqu'à ce que la taille limite du fichier atteigne). La capture est exécutée jusqu'à ce que la limite de fichiers définie ci-dessus soit atteinte. • **Run Capture Until Time Elapsed Reaches** (Exécuter la capture jusqu'à ce que le temps écoulé atteigne l'objectif). La capture s'exécute pendant la durée spécifiée. Si vous entrez la durée sans spécifier d'unités, AsyncOS utilise les secondes par défaut. • **Run Capture Indefinitely** (Exécuter la capture indéfiniment). La capture de paquets continue jusqu'à ce que vous l'arrêtiez manuellement. **Note** La capture peut être arrêtée manuellement à tout moment.
Interfaces	Interfaces à partir lesquelles le trafic sera capturé.
Filters (Filtres)	Les options de filtrage à appliquer lors de la capture de paquets. Le filtrage vous permet de capturer uniquement les paquets requis. Choisissez parmi : • **No Filters** (Aucun filtre). Tous les paquets seront capturés. • **Predefined Filters** (Filtres prédéfinis). Les filtres prédéfinis permettent un filtrage par port et/ou adresses IP. Si ce champ est vide, tout le trafic sera capturé. • **Custom Filter** (Filtre personnalisé). Utilisez cette option si vous connaissez déjà la syntaxe exacte des options de capture de paquets dont vous avez besoin. Utilisez la syntaxe tcpdump standard.

(Facultatif) Envoyez et validez vos modifications de capture de paquets.

Note Lorsque vous modifiez les paramètres de capture de paquets sans valider les modifications, puis que vous démarrez une capture de paquets, AsyncOS utilise les nouveaux paramètres. Cela vous permet d'utiliser les nouveaux paramètres dans la session en cours sans les appliquer pour les futures exécutions de capture de paquets. Les paramètres demeurent en vigueur jusqu'à ce que vous les effaciez.

Étape 3 Cliquez sur **Start Capture** (Commencer la capture). Pour arrêter manuellement une capture en cours, cliquez sur **Stop Capture** (Arrêter la capture).

Gestion des fichiers de capture de paquets

L'appliance enregistre l'activité du paquet capturée dans un fichier et stocke le fichier localement. Vous pouvez envoyer des fichiers de capture de paquets par FTP au service à la clientèle de Cisco à des fins de débogage et de dépannage.

• Téléchargement ou suppression de fichiers de capture de paquets, on page 663

Téléchargement ou suppression de fichiers de capture de paquets

Note Vous pouvez également vous connecter à l'appliance à l'aide du protocole FTP et en récupérant les fichiers de capture de paquets à partir du répertoire des captures.

Étape 1 Choisissez **Support and Help > Packet Capture** (Assistance et aide > Capture de paquets).

Étape 2 Sélectionnez le fichier de capture de paquets que vous souhaitez utiliser dans le volet Manage Packet Capture Files (Gestion des fichiers de capture de paquets). Si ce volet n'est pas visible, aucun fichier de capture de paquet n'a été stocké sur l'appliance.

Étape 3 Cliquez sur **Download File** (Télécharger le fichier) ou sur **Delete Selected Files** (Supprimer les fichiers sélectionnés), comme requis.

Collaboration avec le service d'assistance

• Collecte de renseignements pour un service efficace , on page 663
• Ouverture d'une demande d'assistance technique, on page 664
• Obtenir une assistance pour les appliances virtuelles , on page 664
• Activation de l'accès à distance à l'appliance , on page 665

Collecte de renseignements pour un service efficace

Avant de communiquer avec le service d'assistance :

- Activez les champs de journalisation personnalisés comme décrit dans Bonnes pratiques en matière de résolution des problèmes d'ordre général, on page 633.
- Pensez à effectuer une capture de paquets. Consultez Capture de paquets, on page 661.

Ouverture d'une demande d'assistance technique

Before you begin

- Vérifiez que votre identifiant d'utilisateur Cisco.com est associé à votre contrat de services pour cette appliance. Pour afficher une liste des contrats de service actuellement associés à votre profil Cisco.com, consultez le gestionnaire de profils Cisco.com à l'adresse https://sso.cisco.com/autho/forms/CDClogin.html. Si vous n'avez pas d'ID utilisateur Cisco.com, inscrivez-vous pour l'obtenir.

Vous pouvez utiliser l'appliance pour envoyer une demande d'assistance non urgente à l'assistance client de Cisco. Lorsque l'appliance envoie la demande, elle envoie également sa configuration. L'appliance doit être en mesure d'envoyer des courriels vers Internet pour permettre l'envoi d'une demande d'assistance.

Note Si vous avez un problème urgent, veuillez appeler un centre d'assistance mondiale Cisco.

Étape 1 Choisissez **Support And Help > Contact Technical Support** (Assistance et aide > Contacter l'assistance technique).

Étape 2 (Facultatif) Choisissez des destinataires supplémentaires pour la demande. Par défaut, la demande d'assistance et le fichier de configuration sont envoyés au service à la clientèle de Cisco.

Étape 3 Entrez vos coordonnées.

Étape 4 Entrez les détails du problème.

- Si vous avez déjà un ticket de service à la clientèle pour ce problème, saisissez-le.

Étape 5 Cliquez sur **Envoyer**. Un dossier d'incident est créé avec Cisco.

Obtenir une assistance pour les appliances virtuelles

Si vous déposez une demande d'assistance pour une appliance virtuelle de sécurité de contenu Cisco, vous devez fournir votre numéro de licence virtuelle (VLN), votre numéro de contrat et votre code d'identification de produit (PID).

Vous pouvez identifier votre PID en fonction des licences logicielles s'exécutant sur votre appliance virtuelle, en vous reportant à votre bon de commande ou en consultant le tableau suivant :

Fonctionnalité	PID	Description
Web Security Essentials	WSA-WSE-LIC=	Inclut : • Contrôles d'utilisation du Web • Réputation Web

Fonctionnalité	PID	Description
Web Security Premium	WSA-WSP-LIC=	Inclut : • Contrôles d'utilisation du Web • Réputation Web • Signatures Sophos et Webroot Anti-Malware
Web Security Anti-Malware	WSA-WSM-LIC=	Inclut les signatures Sophos et Webroot Anti-Malware
McAfee Anti-Malware	WSA-AMM-LIC=	—
Cisco Secure Endpoint	WSA-AMP-LIC=	—

Activation de l'accès à distance à l'appliance

L'option d'accès à distance permet à l'assistance client de Cisco d'accéder à distance à votre appliance à des fins d'assistance.

Étape 1 Choisissez **Support And Help > Remote Access** (Assistance et aide > Accès à distance).

Étape 2 Cliquez sur **Enable** (Activer).

Étape 3 Remplissez les options d'accès à distance pour l'assistance client :

Option	Description
Seed String (Chaîne d'amorçage)	Si vous saisissez une chaîne, elle ne doit correspondre à aucune expression secrète existante ou future. La chaîne s'affichera près du haut de la page après que vous aurez cliqué sur Submit (Envoyer). Vous communiquerez cette chaîne à votre agent d'assistance.
Secure Tunnel (Tunnel sécurisé) (recommandé)	Indique si un tunnel sécurisé doit être utilisé pour les connexions d'accès à distance. Lorsque cette option est activée, l'appliance crée un tunnel SSH sur le port spécifié vers le serveur upgrades.ironport.com, sur le port 443 (par défaut). Une fois la connexion établie, l'assistance client de Cisco peut utiliser le tunnel SSH pour obtenir un accès à l'appliance. Une fois le tunnel d'assistance technique activé, il reste connecté à upgrades.ironport.com pendant 7 jours. Après 7 jours, aucune nouvelle connexion ne peut être établie à l'aide du tunnel d'assistance technique, bien que les connexions existantes continuent d'exister et de fonctionner. Le compte d'accès à distance restera actif jusqu'à ce qu'il soit spécifiquement désactivé.
Appliance Serial Number (Numéro de série de l'appliance)	Le numéro de série de l'appliance.

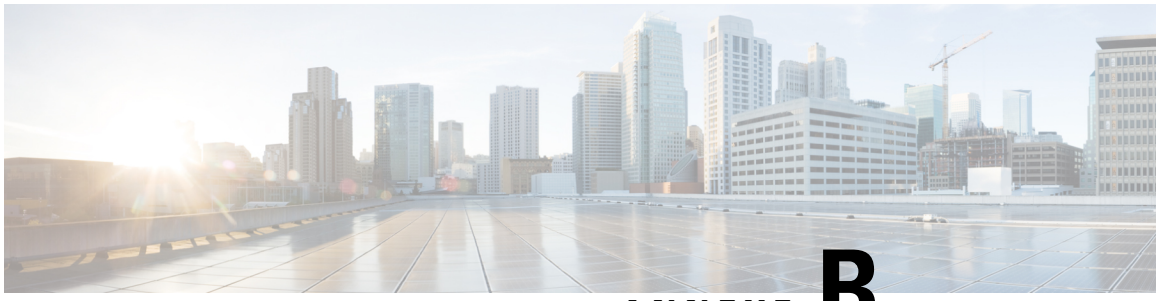
Étape 4 Envoyez et validez vos modifications.

Étape 5 Recherchez la chaîne d'amorçage dans le message de réussite près du haut de la page et notez-la.

Pour des raisons de sécurité, cette chaîne n’est pas stockée sur l’appliance et il n’y a aucun moyen de la retrouver ultérieurement.

Conservez cette chaîne d’amorçage en lieu sûr.

Étape 6 Transmettez la chaîne d’amorçage à votre représentant du service d’assistance.



ANNEXE B

Interface de commande en ligne

Cette rubrique contient les sections suivantes :

Survol de l'interface de commande en ligne

L'interface de ligne de commande (CLI) AsyncOS vous permet de configurer et de surveiller Secure Web Appliance. L'interface de ligne de commande est accessible par SSH sur les interfaces IP configurées avec ces services activés ou par un logiciel d'émulation de terminal sur le port série. Par défaut, SSH est configuré sur le port de gestion.

Les commandes sont appelées en saisissant le nom de la commande avec ou sans arguments. Si vous entrez une commande sans arguments, la commande vous invite à fournir les renseignements requis.

Accès à l'interface de commande en ligne

Vous pouvez vous connecter à l'aide de l'une des méthodes suivantes :

- **Ethernet.** Démarrez une session SSH avec l'adresse IP de Secure Web Appliance. L'adresse IP par défaut est 192.168.42.42. SSH est configuré pour utiliser le port 22.
- **Port série.** Démarrez une session de terminal avec le port de communication de votre ordinateur personnel auquel le câble série est connecté.

Premier accès

Vous pouvez ajouter d'autres utilisateurs avec des niveaux d'autorisation différents après avoir accédé à l'interface de commande en ligne pour la première fois en utilisant le compte **admin**. Pour cela, connectez-vous à l'appliance en saisissant le nom d'utilisateur et la phrase secrète par défaut **admin** :

- Nom d'utilisateur : **admin**
- Phrase secrète : **ironport**

L'Assistant de configuration du système vous invite à modifier la phrase secrète du compte **admin** la première fois que vous vous connectez avec la phrase secrète par défaut.

Vous pouvez également réinitialiser la phrase secrète du compte **admin** à tout moment à l'aide de la commande `passwd`.

Accès ultérieurs

Vous pouvez vous connecter et ouvrir une session sur l'appliance à tout moment en utilisant un nom d'utilisateur et une phrase secrète valides. Notez qu'une liste des tentatives d'accès récentes à l'appareil, réussites et échecs, pour le nom d'utilisateur actuel s'affiche automatiquement lors de la connexion.

Consultez la description de la commande `userconfig` suivante ou Administration des comptes d'utilisateur, on page 580 pour obtenir des renseignements sur la configuration d'utilisateurs supplémentaires.

Utilisation de l'invite de commande

L'invite de commande de niveau supérieur comprend le nom d'hôte complet, suivi du symbole supérieur à (>), suivi d'un espace. Par exemple :

```
example.com>
```

Lors de l'exécution de commandes, vous devez demander votre contribution sur l'interface de ligne de commande. Lorsque l'interface de ligne de commande attend des entrées, l'invite affiche les valeurs par défaut entre crochets (`[ ]`) suivies du symbole supérieur à (>). Lorsqu'il n'y a pas de valeur par défaut, les parenthèses sont vides.

Par exemple :

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

Lorsqu'il existe un paramètre par défaut, il est affiché entre parenthèses dans l'invite de commandes. Par exemple :

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

Lorsqu'un paramètre par défaut est affiché, taper sur la touche de retour équivaut à accepter le paramètre par défaut.

Syntaxe de la commande

En mode interactif, la syntaxe des commandes de l'interface de ligne de commande se compose de commandes uniques sans espace, sans arguments ni paramètres. Par exemple :

```
example.com> logconfig
```

Sélectionner des listes

Lorsque plusieurs choix de saisie s'affichent, certaines commandes utilisent des listes numérotées. Saisissez le numéro de la sélection à l'invite.

Par exemple :

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

Requêtes oui/non

Lorsqu'on doit répondre par oui ou par non, la question est posée avec une valeur par défaut entre parenthèses. Vous pouvez répondre par **Y** (O), **N**, **Yes** (Oui) ou **No** (Non). Le respect de la casse n'est pas important.

Par exemple :

```
Do you want to enable the proxy? [Y]> Y
```

Sous-commandes

Certaines commandes vous donnent la possibilité d'utiliser des directives de sous-commandes telles que `NEW`, `EDIT et DELETE`. Les fonctions `EDIT` et `DELETE` offrent une liste de valeurs précédemment configurées.

Par exemple :

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (172.xxx.xx.xx/xx: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
```

Dans les sous-commandes, appuyez sur Entrée ou Retour à une invite vide pour revenir à la commande principale.

Quitter les sous-commandes

Vous pouvez utiliser le raccourci clavier Ctrl+C à tout moment dans une sous-commande pour la quitter et retourner immédiatement au niveau supérieur de l'interface de ligne de commande.

Historique des commandes

L'interface de ligne de commande conserve un historique de toutes les commandes saisies au cours d'une session. Utilisez les flèches Haut et Bas du clavier ou les combinaisons de touches Ctrl+P et Ctrl+N pour faire défiler la liste des commandes récemment utilisées.

Commandes complémentaires

L'interface de ligne de commande d'AsyncOS prend en charge les commandes complémentaires. Vous pouvez entrer les premières lettres de certaines commandes, suivies de la touche de tabulation, et l'interface de ligne de commande complète la chaîne. Si les lettres que vous avez saisies ne sont pas uniques parmi les commandes, l'interface de ligne de commande « affine » l'ensemble. Par exemple :

```
example.com> set (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
example.com> sethostname
```

Validation des modifications de configuration à l'aide de l'interface CLI

- De nombreuses modifications de configuration ne prennent effet que lorsque vous les validez.
- La commande `commit` vous permet de modifier les paramètres de configuration pendant que les autres opérations se déroulent normalement.
- Pour réussir la validation des modifications, vous devez vous trouver au niveau de l'invite de commande de niveau supérieur. Tapez **Return** (Retour) dans une invite vide pour monter d'un niveau dans la hiérarchie de ligne de commande.
- Les modifications de configuration qui n'ont pas été validées sont enregistrées, mais ne prennent effet que lorsque vous exécutez la commande `commit`. Cependant, toutes les commandes ne nécessitent pas l'exécution de la commande `commit`. La sortie de la session CLI, l'arrêt du système, le redémarrage, un échec ou l'exécution de la commande `clear` efface les modifications qui n'ont pas encore été validées.
- Les modifications ne sont réellement validées que lorsque vous recevez une confirmation et un horodatage.

Commandes générales de l'interface de ligne de commande

Cette section décrit quelques commandes de base que vous pouvez utiliser dans une session CLI typique, telles que la validation et l'effacement des modifications.

Exemple d'interface de ligne de commande : validation des modifications de configuration

La saisie de commentaires après la commande de validation est facultative.

```
example.com> commit

Please enter some comments describing your changes:
[]> Changed "psinet" IP Interface to a different IP address
Changes committed: Wed Jan 01 12:00:01 2007
```

Exemple d'interface de ligne de commande : effacement des modifications de configuration

La commande clear efface toutes les modifications apportées à la configuration de l'appliance depuis la dernière commande de validation ou d'effacement.

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Wed Jan 01 12:00:01 2007
example.com>
```

Exemple d'interface de ligne de commande : sortie de la session d'interface de commande en ligne

La commande exit vous déconnecte de l'application CLI. Les modifications de configuration qui n'ont pas été validées sont effacées.

```
example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> y
```

Exemple d'interface de ligne de commande : demande d'aide sur l'interface de commande en ligne

La commande `help` répertorie toutes les commandes d'interface de ligne de commande disponibles et donne une brève description de chaque commande. La commande `help` peut être appelée en tapant aide ou un seul point d'interrogation (?) dans l'invite de commande.

```
example.com> help
```

En outre, vous pouvez accéder à l'aide pour une commande spécifique en entrant **`help`** `commandname`.

Thèmes connexes

- Commandes de l'interface de ligne de commande Secure Web Appliance, on page 671

Commandes de l'interface de ligne de commande Secure Web Appliance

L'interface de ligne de commande Secure Web Appliance prend en charge un ensemble de proxy et de commandes UNIX pour accéder au système, le mettre à niveau et administrer le système.

Note Les commandes de l'interface de ligne de commande ne sont pas toutes applicables ou disponibles dans tous les modes de fonctionnement (connecteur de sécurité Web standard et infonuagique).

adminaccessconfig

Vous pouvez configurer Secure Web Appliance pour avoir des exigences d'accès plus strictes pour les administrateurs qui se connectent à l'appliance, et vous pouvez spécifier une valeur de délai d'inactivité. Reportez-vous à Paramètres de sécurité supplémentaires pour l'accès à l'appliance, on page 587 et à Accès au réseau de l'utilisateur, on page 589 pour en savoir davantage.

advancedproxyconfig

Configurez les options avancées de proxy Web; les sous-commandes sont :

`AUTHENTICATION` – Options de configuration de l'authentification :

- `When would you like to forward authorization request headers to a parent proxy` (Quand souhaitez-vous transférer les en-têtes de demande d'autorisation à un proxy parent)
- `Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog` (Entrez le domaine d'autorisation de proxy à afficher dans la boîte de dialogue d'authentification de l'utilisateur final)
- `Would you like to log the username that appears in the request URI` (Voulez-vous connecter le nom d'utilisateur qui apparaît dans l'URI de la demande?)
- `Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed)` [Si l'attribut Group Membership est utilisé pour des recherches dans l'annuaire dans l'interface utilisateur Web (lorsqu'il n'est pas utilisé, les groupes vides et les groupes avec des attributs d'appartenance différents seront affichés)]
- `Would you like to use advanced Active Directory connectivity checks?` (Voulez-vous utiliser les vérifications avancées de la connectivité Active Directory?)
- `Would you like to allow case insensitive username matching in policies?` (Voulez-vous autoriser la mise en correspondance de noms d'utilisateurs non sensible à la casse dans les politiques?)
- `Would you like to allow wild card matching with the character * for LDAP group names?` (Voulez-vous autoriser la correspondance de caractères génériques avec le caractère * pour les noms de groupe LDAP?)
- `Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8]` (Saisissez le jeu de caractères utilisé par les clients pour l'authentification de base [ISO-8859-1/UTF-8])
- `Would you like to enable referrals for LDAP?` (Voulez-vous activer les recommandations pour LDAP?)
- `Would you like to enable secure authentication?` (Voulez-vous activer l'authentification sécurisée?)
- `Enter the hostname to redirect clients for authentication` (Saisissez le nom d'hôte pour rediriger les clients pour l'authentification)

- `Enter the surrogate timeout for user credentials` (Saisissez le délai d'expiration de substitution pour les informations d'authentification de l'utilisateur)
- `Saisissez le délai d'expiration de substitution pour les informations d'authentification de l'ordinateur`
- `Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability` (Saisissez le délai d'expiration de substitution si le trafic a été autorisé en raison de l'indisponibilité du service d'authentification)
- `Enter re-auth on request denied option [disabled / embedlinkinblockpage]` [Saisissez l'option de réauthentification sur demande refusée (disabled / embedLinkinblockpage)]
- `Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication?` (Voulez-vous envoyer l'en-tête Negotiate avec l'en-tête NTLM pour l'authentification NTLMSSP?)
- `Configure username and IP address masking in logs and reports` (Configurer le masquage du nom d'utilisateur et de l'adresse IP dans les journaux et les rapports)
- `Timeout to enable/disable local Auth cache` (Délai d'expiration pour activer/désactiver le cache d'authentification local).

  Vous pouvez utiliser cette option de l'interface de ligne de commande pour activer ou désactiver le cache d'authentification immédiate du processus proxy. Le temps défini est en secondes. Par défaut, cette option est activée et définie pendant 30 secondes. Ce délai doit être plus court que le temps de substitution IP.

`CACHING` – Mode de mise en cache du proxy; choisissez une option :

- `Safe Mode` (Mode sans échec)
- `Optimized Mode` (Mode optimisé)
- `Aggressive Mode` (Mode agressif)
- `Customized Mode` (Mode personnalisé)

  Voir aussi Choix du mode de mise en mémoire cache du proxy Web, on page 78.

`DNS` – Options de configuration du DNS :

- `Enter the URL format for the HTTP 307 redirection on DNS lookup failure` (Saisissez le format de l'URL pour la redirection HTTPno-break space - U+00A0307 en cas d'échec de la recherche DNS)
- `Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure?` (Voulez-vous que le proxy envoie une redirection HTTP 307 en cas d'échec de la recherche DNS?)
- `Voulez-vous que le proxy ne bascule pas automatiquement vers les résultats du DNS lorsque le proxy en amont (homologue) ne répond pas?`
- `Do you want to disable IP address in Host Header` (Voulez-vous désactiver l'adresse IP dans l'en-tête de l'hôte)
- `Find web server by:` (Trouvez un serveur Web par :)

  `0 = Always use DNS answers in order` (0=Toujours utiliser les réponses DNS dans l'ordre)

  `1 = Utiliser l'adresse fournie par le client, puis les DNS`

  `2 = Limited DNS usage` (2 = Utilisation DNS limitée)

`3 = Very limited DNS usage` (3 = Utilisation DNS très limitée)

La valeur par défaut est égale à 0. Pour les options 1 et 2, DNS sera utilisé si la réputation de sites Web est activée. Pour les options 2 et 3, les DNS seront utilisés pour les demandes de proxy explicites, s'il n'y a pas de proxy en amont ou en cas d'échec du proxy en amont configuré. Pour toutes les options, le DNS sera utilisé lorsque les adresses IP de destination sont utilisées dans l'appartenance à la politique.

`EUN` – Paramètres de notification de l'utilisateur final :

- `Choose` (Choisissez :)

  `1. Refresh EUN pages` (Actualiser les pages EUN)

  `2. Use Custom EUN pages` (Utiliser des pages EUN personnalisées)

  `3. Use Standard EUN pages` (Utiliser les pages standard EUN)

- `Would you like to turn on presentation of the User Acknowledgement page?` (Voulez-vous activer la présentation de la page de confirmation de l'utilisateur?)

Voir aussi Contrat d'utilisation du proxy Web, on page 86 et Survol des notifications envoyées à l'utilisateur final, on page 371.

`NATIVEFTP` – Configuration FTP native :

- `Would you like to enable FTP proxy?` (Voulez-vous activer le proxy FTP?)
- `Enter the ports that FTP proxy listens on` (Saisissez les ports sur lesquels le proxy FTP écoute)
- `Enter the range of port numbers for the proxy to listen on for passive FTP connections` (Saisissez la plage de numéros de port sur laquelle le proxy doit entendre les connexions FTP passives)
- `Enter the range of port numbers for the proxy to listen on for active FTP connections` (Saisissez la plage de numéros de port sur laquelle le proxy doit entendre les connexions FTP actives)
- `Enter the authentication format :` (Entrez le format d'authentification :)

  `1. Check Point`

  `2. No Proxy Authentication` (Aucune authentification du proxy)

  `3. Raptor`

- `Would you like to enable caching?` (Voulez-vous activer la mise en cache?)
- `Would you like to enable server IP spoofing?` (Voulez-vous activer l'usurpation d'adresses IP du serveur?)
- `Would you like to enable client IP spoofing?`(Voulez-vous activer l'usurpation d'adresses IP du client?)
- `Would you like to pass FTP server welcome message to the clients?` (Voulez-vous transmettre le message de bienvenue du serveur FTP aux clients?)
- `Enter the max path size for the ftp server directory` (Entrez la taille de chemin maximale pour le répertoire du serveur FTP)

Voir aussiSurvol des services proxy FTP, on page 92.

`FTPOVERHTTP` – Options FTP sur HTTP :

- `Enter the login name to be used for anonymous FTP access` (Saisissez le nom de connexion à utiliser pour l'accès FTP anonyme)
- `Enter the password to be used for anonymous FTP access` (Saisissez le mot de passe à utiliser pour l'accès FTP anonyme)

Voir aussi Survol des services proxy FTP, on page 92.

`Highperformance` (Hautes performances) : active et désactive le mode haute performance.

`HTTPS` – Options liées à HTTPS :

- `HTTPS URI Logging Style - fulluri or stripquery` (Style de journalisation URI HTTPS - fulluri ou stripquery)
- `Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose?` (Voulez-vous déchiffrer les requêtes HTTPS transparentes non authentifiées à des fins d'authentification?)
- `Would you like to decrypt HTTPS requests for End User Notification purpose?` (Souhaitez-vous déchiffrer les demandes HTTPS à des fins de notification à l'utilisateur final?)
- `Action to be taken when HTTPS servers ask for client certificate during handshake:` (Action à entreprendre lorsque les serveurs HTTPS demandent un certificat client lors de l'établissement de liaison :)
  1. `Pass through the transaction` (Transmettre la transaction)
  2. `Reply with certificate unavailable` (Réponse avec certificat non disponible)
- `Do you want to enable server name indication (SNI) extension?` [Voulez-vous activer l'extension SNI (Server Name Indication)?]
- `Do you want to enable automatic discovery and download of missing Intermediate Certificates?` (Voulez-vous activer la découverte et le téléchargement automatiques des certificats intermédiaires manquants?)
- `Do you want to enable session resumption?` (Voulez-vous activer la reprise de session?)

Voir aussi Survol de la création de politiques de déchiffrement pour contrôler le trafic HTTPS, on page 279.

`SCANNING` – Options d'analyse :

- `Would you like the proxy to do malware scanning all content regardless of content type` (Voulez-vous que le proxy analyse tout le contenu contre les programmes malveillants, quel que soit le type de contenu?)
- `Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds` [Saisissez le temps d'attente d'une réponse d'un moteur d'analyse contre les programmes malveillants (Sophos, McAfee ou Webroot), en secondes]
- `Do you want to disable Webroot body scanning?` (Voulez-vous désactiver l'analyse du corps Webroot?)

Voir aussi Survol de l'analyse à la recherche de programmes malveillants , on page 307 et Survol de l'analyse du trafic sortant, on page 295.

`SCANNERS` – Exclut les types MIME de l'analyse par le moteur Cisco Secure Endpoint . Pour utiliser la sous-commande analyseurs, vous devez désactiver la fonction de « analyse adaptative ». À l'aide de cette

sous-commande, vous pouvez ajouter les types MIME qui n'ont pas besoin d'être analysés par le moteur Cisco Secure Endpoint pour augmenter les performances d'analyse. Les options de type MIME par défaut sont « image/ALL et text/ALL ».

Pour ajouter les types MIME, vous devez les ajouter après les options par défaut. Par exemple, si vous souhaitez ajouter les types MIME vidéo et audio, le format doit être :

« image/ALL et text/ALL vidéo/ALL audio/ALL »

PROXYCONN – Gère la liste des agents utilisateurs qui ne peuvent pas accepter l'en-tête de connexion proxy. Les entrées de la liste sont interprétées comme des expressions régulières dans le langage Flex (Fast Lexical Analyzer). Un agent utilisateur sera mis en correspondance si une sous-chaîne de celui-ci correspond à une expression régulière de la liste.

- Choisissez l'opération que vous souhaitez effectuer :

  `NEW - Add an entry to the list of user agents` (NOUVEAU - Ajouter une entrée à la liste des agents utilisateurs)

  `DELETE - Remove an entry from the list` (SUPRIMER - Supprimer une entrée de la liste)

CUSTOMHEADERS – Gérer les en-têtes de demande personnalisés pour des domaines spécifiques.

- Choisissez l'opération que vous souhaitez effectuer :

  `DELETE - Delete entries` (SUPPRIMER - Supprimer des entrées)

  `NEW - Add new entries` (NOUVEAU - Ajouter de nouvelles entrées)

  `EDIT - Edit entries` (MODIFIER - Modifier les entrées)

Voir aussi Ajout d'en-têtes personnalisés aux demandes Web, on page 81.

MISCELLANEOUS (DIVERS) - Paramètres divers liés au proxy :

- `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)` [Voulez-vous que le proxy réponde aux contrôles de l'intégrité des commutateurs de couche 4 (toujours activé si WSA est en mode transparent sur la couche 4)]
- `Voulez-vous que le proxy effectue un ajustement dynamique de la taille de la fenêtre de réception TCP?`
- `Would you like proxy to perform dynamic adjustment of TCP send window size?` (Voulez-vous que le proxy effectue un ajustement dynamique de la taille de la fenêtre d'envoi TCP?)
- `Do you want to filter non-HTTP responses` (Voulez-vous filtrer les réponses non HTTP?)

  `(Non-HTTP responses are filtered by default.Enter` **`N`** `if you want to allow non-HTTP responses via proxy)` (Les réponses non HTTP sont filtrées par défaut. Saisissez N si vous souhaitez autoriser les réponses non HTTP par l'intermédiaire d'un proxy)
- `Enable caching of HTTPS responses` (Activez la mise en cache des réponses HTTPS)
- `Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds)` [Saisissez le délai d'inactivité minimal pour la vérification du proxy en amont qui ne répond pas (en secondes)]
- `Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)` [Saisissez le délai d'inactivité maximal pour la vérification du proxy en amont qui ne répond pas (en secondes)]
- `Mode of the proxy:` (Mode du proxy :)

1. `Explicit forward mode only` (Mode de transfert explicite uniquement)
2. `Transparent mode with L4 Switch or no device for redirection` (Mode transparent avec commutateur de couche 4 ou aucun périphérique pour la redirection)
3. `Transparent mode with WCCP v2 Router for redirection` (Mode transparent avec routeur WCCP v2 pour la redirection)

- Usurpation de l'adresse IP du client par le proxy :
  1. `Enable for all requests` (Activer pour toutes les demandes)
  2. `Enable for transparent requests only` (Activer pour les demandes transparentes uniquement)
- `Do you want to pass HTTP X-Forwarded-For headers?` (Voulez-vous transmettre les en-têtes HTTP X-Forwarded-For?)
- `Do you want to enable server connection sharing?` (Voulez-vous activer le partage de la connexion du serveur?)
- `Would you like to permit tunneling of non-HTTP requests on HTTP ports?` (Voulez-vous autoriser la tunnellisation des requêtes non HTTP sur les ports HTTP?)
- `Would you like to block tunneling of non-SSL transactions on SSL Ports?` (Voulez-vous bloquer la tunnellisation des transactions non SSL sur les ports SSL?)
- `Voulez-vous que le proxy consigne les valeurs des en-têtes X-Forwarded-For à la place des adresses IP de connexion entrante?`
- `Do you want proxy to throttle content served from cache?` (Voulez-vous que le proxy limite le contenu servi à partir du cache?)
- `Voulez-vous que le proxy utilise les adresses IP client des en-têtes X-Forwarded-For`
- `Do you want to forward TCP RST sent by server to client?` (Voulez-vous transférer le RST du serveur TCP envoyé par le serveur au client?)
- `Voulez-vous activer la vérification de l'intégrité du proxy WCCP?`
- `Do you want to enable URL lower case conversion for velocity regex?` (Voulez-vous activer la conversion d'URL en minuscules pour l'expression régulière de vitesse?)

Voir aussi Utilisation de l'interface de données P2 pour les données de proxy Web , on page 42 et Configuration des paramètres du proxy Web, on page 73.

`socks` : options de proxy SOCKS :

- `Would you like to enable SOCKS proxy` (Voulez-vous activer le proxy SOCKS?)
- `Proxy Negotiation Timeout` (Délai d'expiration de la négociation du proxy)
- `UDP Tunnel Timeout` (Délai d'expiration du tunnel UDP)
- `SOCKS Control Ports` (Ports de contrôle SOCKS)
- `UDP Request Ports` (Ports de demande UDP)

Voir aussi Utilisation de l'interface de données P2 pour les données de proxy Web , on page 42 et Services proxy SOCKS, on page 94.

`CONTENT-ENCODING` – Autoriser et bloquer les types de codage de contenu.

Types d'encodage de contenu actuellement autorisés : compress, deflate, gzip

Types d'encodage de contenu actuellement bloqués : S.O.

Pour modifier le paramètre d'un type d'encodage de contenu spécifique, sélectionnez une option :

1. compress

2. deflate

3. gzip

[1]>

Le type d'encodage « compress » est actuellement autorisé

Voulez-vous le bloquer? [N]>

Note La commande **centralauthcache** s'applique aux appareils compatibles avec les performances élevées et pour améliorer les performances du cache d'authentification.

adminaccessconfig

Vous pouvez configurer Secure Web Appliance pour avoir des exigences d'accès plus strictes pour les administrateurs qui se connectent à l'appliance.

configuration d'alerte

Spécifiez les destinataires des alertes et définissez les paramètres d'envoi des alertes du système.

authcache

Vous permet de supprimer une ou toutes les entrées (utilisateurs) du cache d'authentification. Vous pouvez également répertorier tous les utilisateurs actuellement inclus dans le cache d'authentification.

Note Lorsque *centralauthcache* est activé, la commande *authcache* n'affiche pas le nom d'utilisateur authentifié ISE. Pour obtenir les informations sur l'utilisateur d'ISE, utilisez la commande *isedata*.

bwcontrol

Débogue la fonctionnalité de contrôle de la bande passante.

- **bwcontrol listnips :** Affiche la liste de tous les canaux de contrôle de bande passante actifs sur Secure Web Appliance.
- **bwcontrol monitor <numéro du canal>** : pour afficher la bande passante mesurée pour le canal de transmission donné, une fois toutes les cinq secondes.

À partir d'AsyncOS 14.5, les journaux de proxy en mode Trace (Suivi) sont affichés par défaut.

Terminologie

- `URLBW` : Contrôle de la bande passante appliqué par catégorie d'URL de politique d'accès
- `OverallBW` : Contrôle de la bande passante appliqué par le quota d'activité Web globale de la politique d'accès.
- `OverallMediaBW` : Contrôle de la bande passante appliqué par la limite de bande passante globale.
- `AVCPerUserBW` : Contrôle de la bande passante appliqué par la limite de bande passante AVC.

certconfig

`SETUP` : Configure les certificats de sécurité et les clés.

`OCSPVALIDATION` : Active/désactive la validation OCSP du certificat pendant le téléchargement.

`OCSPVALIDATION_FOR_SERVER_CERT` : Active la validation OCSP pour les certificats de serveur Active la validation OCSP pour les certificats de serveur

clear

Efface les modifications de configuration en attente depuis la dernière validation.

clientconnections

Affiche les détails de la connexion lorsque le nombre maximal de connexions par client est activé. Les détails comprennent l'adresse IP du client et le nombre de connexions.

Choisissez l'opération que vous souhaitez effectuer :

- `LIST` : Répertorie toutes les entrées de la base de données de cstat
- `SEARCH` : Recherche une entrée dans la base de données de cstat

commit

Valide les modifications en attente à la configuration du système.

configbackup

Enregistre le fichier de configuration de sauvegarde et l'envoie à un serveur de sauvegarde distant par FTP ou SCP

csidconfig

Vous pouvez configurer différents paramètres de la fonctionnalité Cisco Success Network sur l'appliance en ce qui concerne la publication des données de télémesure sur le portail d'échange de services de sécurité.

Les sous-commandes sont :

- `OPT_OUT` : active/désactive la transmission des données de télémesure CSI
- `CSIDATAPUSHINTERVAL` : configure l'intervalle de temps de transmission des données de télémesure.

createcomputerobject

Crée un objet ordinateur à l'emplacement que vous spécifiez.

curl

Envoyez une demande cURL directement à un serveur Web ou à un serveur Web par l'intermédiaire d'un proxy, avec les en-têtes HTTP de demande et de réponse renvoyés pour vous permettre de déterminer la raison du chargement d'une page Web.

Note Cette commande est réservée à l'usage de l'administrateur ou de l'opérateur, sous la supervision du service d'assistance technique de Cisco.

Les sous-commandes sont :

- `DIRECT` : accès URL direct
- `APPLIANCE` : URL d'accès par le biais de l'appliance

datasecurityconfig

Définit une taille minimale de corps de demande en dessous de laquelle les demandes de téléchargement ne sont pas analysées par les filtres de sécurité des données de Cisco.

date

Affiche la date actuelle. Exemple :

```
Thu Jan 10 23:13:40 2013 GMT
```

diagnostic

Sous-commandes liées au proxy et à la création de rapports :

`NET` : utilitaire de diagnostic réseau

Cette commande est obsolète; utilisez packetcapture pour capturer le trafic réseau sur l'appliance.

`PROXY` : utilitaire de débogage de proxy

Choisissez l'opération que vous souhaitez effectuer :

- `SNAP` : prend un instantané du proxy
- `OFFLINE` : met le proxy hors ligne (par le biais de WCCP)
- `RESUME` : reprend le trafic proxy (par le biais de WCCP)
- `CACHE` : efface le cache du proxy

`proxyscannermap` : cette commande affiche le mappage de PID entre chaque proxy et le processus d'analyseur correspondant.

`REPORTING` : utilitaires de rapport

Le système de rapports est actuellement activé.

Choisissez l'opération que vous souhaitez effectuer :

- `DELETDB` : réinitialise la base de données de rapports

- `DISABLE` : désactive le système de rapports.
- `DBSTATS` : répertorie la base de données et les fichiers d'exportation (affiche la liste des fichiers et des dossiers non traités dans les dossiers export_files et always_onbox.)
- `DELETEEXPORTDB` : supprime les fichiers d'exportation (supprime tous les fichiers et dossiers non traités dans les dossiers export_files et always_onbox.)
- `DELETEJOURNAL` : supprime les fichiers de journal (supprime tous les aclog_journal_files.)

dnsconfig

Configure les paramètres du DNS.

Choisissez l'opération que vous souhaitez effectuer :

- `NEW` : ajoute un nouveau serveur.
- `EDIT` : modifie un serveur.
- `DELETE` : supprime un serveur.
- `SETUP` : configure les paramètres généraux.
- `SEARCH` : configure la liste de recherche de domaines DNS.

```
[]> setup
```

```
Do you want to enable Secure DNS? [N]> Yes
```
(Voulez-vous activer le DNS sécurisé? [N]> Oui)

dnsflush

Purge des entrées DNS sur l'appliance.

etherconfig

Configure les connexions du port Ethernet.

Choisissez l'opération que vous souhaitez effectuer :

- `MEDIA` : affiche et modifie les paramètres de supports Ethernet.
- `PAIRING` : affiche et configure l'appairage de cartes réseau.
- `VLAN` : affiche et configure les VLAN.
- `MTU` : affiche et configure la MTU.

externaldlpconfig

Définit une taille minimale de corps de demande en dessous de laquelle les demandes de téléchargement ne sont pas analysées par le serveur DLP externe.

externaldlpconfig

Définit une taille minimale de corps de demande en dessous de laquelle les demandes de téléchargement ne sont pas analysées par le serveur DLP externe.

featurekey

Soumet des clés valides pour activer les fonctionnalités sous licence.

featurekeyconfig

Vérifie et met à jour automatiquement les clés de fonctionnalité.

fipsconfig

SETUP : active/désactive la conformité FIPS 140-2 et le chiffrement des paramètres sensibles critiques (CSP). Notez qu'un redémarrage immédiat sera nécessaire.

FIPSCHECK : vérifie la conformité du mode FIPS. Indique si les divers certificats et services sont conformes aux normes FIPS.

Voir Conformité à la norme FIPS, on page 603 pour de plus amples informations.

grep

Recherche dans les fichiers d'entrée nommés les lignes contenant une correspondance au modèle donné.

gathererdconfig

Configure la fonctionnalité d'interrogation entre l'appliance et le serveur d'authentification.

help

Renvoie une liste de commandes.

httppatchconfig

Active ou désactive les demandes de correctifs HTTP sortantes. La valeur par défaut est enable (activer).

http2

Active ou désactive les configurations HTTP 2.

iccm_message

Efface le message de l'interface Web et de l'interface de ligne de commande indiquant quand ce Secure Web Appliance est géré par une appliance de gestion de la sécurité (Series M).

ifconfig ou interfaceconfig

Configure et gère les interfaces réseau, notamment M1, P1 et P2. Affiche les interfaces actuellement configurées et fournit un menu des opérations pour créer, modifier ou supprimer des interfaces.

iseconfig

Affiche les paramètres de configuration ISE actuels; indiquez une opération de configuration ISE à effectuer :

`ISE RECONCILIATION TIME SETUP` — Configure l'heure de rapprochement de Cisco ISE. Pour redémarrer le processus installé automatiquement, définissez l'heure au format HH::MM dans les 24 heures suivant la configuration d'ISE. Après un redémarrage, le téléchargement en bloc a lieu.

```
Choose the operation you want to perform:
- Schedule ISE Restart Time in HH:MM format.
- Modify cache timeout for ISE users. Specify a timeout value in hours, upto 24 hours
```

Par défaut, la valeur de l'option 1 est 00 h 00 à minuit.

isedata

Précisez une opération liée aux données ISE :

`statistics` : affiche l'état du serveur et les statistiques ISE du serveur.

`cache` : affiche le cache ISE ou vérifiez une adresse IP :

`sgts` : affiche le tableau des balises SGT ISE.

`groups` : affiche le tableau des groupes ISE.

Si VDI est mis en œuvre, les sous-commandes `show` et `checkip` sous la commande principale `cache` affichent plus de détails. La sous-commande `show` affiche les détails sur la plage de ports et la sous-commande `checkip` affiche les détails sur l'utilisateur VDI, tels que l'adresse IP, le nom, la plage de ports, etc.

```
[]> cache

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
```

last

Répertorie les informations utilisateur spécifiques à l'utilisateur, qui comprennent les tty et les hôtes, dans l'ordre inverse du temps ou répertorie les utilisateurs connectés à une date et à une heure spécifiées.

loadconfig

Charge un fichier de configuration système.

logconfig

Configure l'accès aux fichiers journaux.

mailconfig

Envoie le fichier de configuration actuel à l'adresse spécifiée.

maxhttpheadersize

Définit la taille maximale de l'en-tête HTTP ou la taille de l'URL pour les demandes de proxy; saisissez la valeur en octets ou ajoutez un K au nombre pour indiquer les kilo-octets.

Le suivi des politiques peut échouer pour un utilisateur qui appartient à un grand nombre de groupes d'authentification. Il peut également échouer si la taille de l'en-tête de la réponse HTTP ou la taille de l'URL est supérieure à la « taille maximale d'en-tête » actuelle. L'augmentation de cette valeur peut réduire ces échecs. La valeur minimale est de 32 Ko; la valeur par défaut est de 32 Ko; La valeur maximale est de 1 024 Ko.

modifyauthhelpers

Utilisez cette commande pour configurer le nombre d'assistants d'authentification Kerberos entre 5 et 21 pour BASIC, NTLMSSP et NEGO.

musconfig

Utilisez cette commande pour activer Secure Mobility et configurer l'identification des utilisateurs à distance, soit par adresse IP, soit par intégration dans une ou plusieurs appliances Cisco Adaptive Security Appliance.

Note Les modifications apportées à l'aide de cette commande entraînent le redémarrage du proxy Web.

musstatus

Utilisez cette commande pour afficher les informations relatives à Secure Mobility lorsque Secure Web Appliance est intégré à une appliance ASA.

Cette commande affiche les informations suivantes :

- L'état de la connexion Secure Web Appliance avec chaque appliance ASA.
- La durée de la connexion Secure Web Appliance avec chaque appliance ASA en minutes.
- Le nombre de clients distants de chaque appliance ASA.
- Le nombre de clients distants desservis, qui est défini comme le nombre de clients distants qui ont transmis du trafic par l'intermédiaire de Secure Web Appliance.
- Le nombre total de clients distants.

networktuning

Secure Web Appliance utilise plusieurs tampons et algorithmes d'optimisation pour gérer des centaines de connexions TCP simultanément, offrant des performances élevées pour le trafic Web typique, c'est-à-dire les connexions HTTP de courte durée.

Dans certaines situations, par exemple en cas de téléchargements fréquents de fichiers volumineux (plus de 100 Mo), des tampons plus grands peuvent fournir de meilleures performances par connexion. Cependant, l'utilisation globale de la mémoire augmentera et, par conséquent, toute augmentation de la mémoire tampon doit correspondre à la mémoire disponible sur le système.

Les variables d'espace d'envoi et de réception représentent les tampons utilisés pour stocker les données pour les communications sur une connexion TCP donnée. Les variables send- et received-auto sont utilisées pour activer et désactiver l'algorithme de réglage automatique de FreeBSD pour le contrôle dynamique de la taille de la fenêtre. Ces deux paramètres sont appliqués directement dans le noyau de FreeBSD.

Lorsque `SEND_AUTO` et `RECV_AUTO` sont activés, le système ajuste la taille de la fenêtre de manière dynamique en fonction de la charge du système et des ressources disponibles. Sur un Secure Web Appliance légèrement chargé, le système tente de maintenir une grande taille de fenêtre pour réduire la latence par transaction. La valeur maximale de la taille de fenêtre réglée dynamiquement dépend du nombre configuré de grappes mbuf, qui à son tour dépend de la RAM totale disponible sur le système. À mesure que le nombre total de connexions client augmente, ou lorsque les ressources de tampon réseau disponibles se raréfient, le système ajuste la taille de la fenêtre pour éviter de perdre toutes les ressources de tampon réseau à cause du trafic sur le proxy.

Consultez Problèmes de vitesse de chargement/téléchargement, on page 640 pour en savoir plus sur l'utilisation de cette commande.

Les sous-commandes `networktuning` sont :

SENDSPACE : Taille de la mémoire tampon de l'espace d'envoi TCP; la plage est comprise entre 8 192 et 131 072 octets; la valeur par défaut est de 16 000 octets.

RECVSPACE : Taille de la mémoire tampon de l'espace de réception TCP; la plage est comprise entre 8192 et 131072 octets; la valeur par défaut est de 32 768 octets.

SEND-AUTO : Active/désactive le réglage automatique de l'envoi TCP; 1 = activé, 0 = éteint; la valeur par défaut est désactivée. Si vous activez le réglage automatique de l'envoi TCP, veillez à utiliser `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size?` (advancedproxyconfig > miscellaneous > Souhaitez-vous que le proxy effectue un réglage dynamique de la taille de la fenêtre d'envoi TCP?) pour désactiver le réglage automatique de la mémoire tampon d'envoi.

RECV-AUTO : Active/désactive le réglage automatique de la réception du protocole TCP; 1 = activé, 0 = éteint; la valeur par défaut est désactivée. Si vous activez le réglage automatique de la réception TCP, assurez-vous d'utiliser `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size?` (Souhaitez-vous que le proxy effectue un réglage dynamique de la taille de la fenêtre de réception TCP?) pour désactiver le réglage automatique de la mémoire tampon de réception.

MBUF CLUTER COUNT : Modifie le nombre de grappes mbuf disponibles; La plage de valeurs acceptables est comprise entre 98 304 et 1 572 864. La valeur doit varier en fonction de la mémoire système installée, en utilisant ce calcul : 98 304 * (X/Y) où X représente les gigaoctets de RAM sur le système et Y 4 Go. Par exemple, avec 4 Go de RAM, la valeur recommandée est 98 304 * (4/4) = 98 304. Une mise à l'échelle linéaire est recommandée à mesure que la RAM augmente.

SENDBUF-MAX : Spécifie la taille maximale de la mémoire tampon d'envoi; la plage est de 131 072 octets à 2 097 152 octets; la valeur par défaut est de 1 Mo (1 048 576 octets).

RECVBUF-MAX : Spécifiez la taille maximale de la mémoire tampon de réception; la plage est de 131 072 octets à 2 097 152 octets; la valeur par défaut est de 1 Mo (1 048 576 octets).

CLEAN-FIB-1 : Supprime toutes les entrées M1/M2 de la table de routage des données – essentiellement, activez la séparation entre le plan de contrôle et le plan de données. En d'autres termes, cela empêche tout processus du plan de données d'envoyer des données sur l'interface M1 lorsque le « routage séparé » est activé. Les processus du plan de données sont ceux pour lesquels l'option d'utilisation de la table de routage des données est activée ou qui acheminent strictement du trafic non lié à la gestion. Les processus du plan de commande peuvent toujours envoyer des données par les interfaces M1 ou P1.

Après toute modification de ces paramètres, assurez-vous de valider vos modifications et de redémarrer l'appliance.

Caution Utilisez cette commande uniquement si vous en comprenez les ramifications. Nous vous recommandons d'utiliser ce produit uniquement avec les conseils du service d'assistance technique de Cisco.

nslookup

Interroge les serveurs de noms de domaine Internet pour obtenir des renseignements à propos d'hôtes et de domaines précisés ou pour imprimer une liste des hôtes d'un domaine.

ntpconfig

Configure les serveurs NTP. Affiche les interfaces actuellement configurées et fournit un menu des opérations pour ajouter, supprimer ou définir l'interface de l'adresse IP de laquelle les requêtes NTP doivent provenir.

packetcapture

Intercepte et affiche le protocole TCP/IP et les autres paquets transmis ou reçus sur le réseau auquel l'appliance est reliée.

passwd

Définit la phrase secrète.

pathmtudiscovery

Active ou désactive Path MTU Discovery.

Vous pouvez désactiver Path MTU Discovery si vous avez besoin de la fragmentation des paquets.

ping (envoyer un message Ping)

Envoie une demande ECHO ICMP à l'hôte ou à la passerelle spécifiés.

process_status

Affiche la liste des processus actifs de l'appliance.

Note Cette commande est disponible uniquement en mode administrateur

proxyconfig <enable | disable>

Active ou désactive le proxy Web.

proxystat

Affiche les statistiques de proxy Web.

quit, q, exit

Termine un processus ou une session actif.

quotaquery

Pour vérifier ou réinitialiser le volume et l'heure utilisés par une catégorie.

Choisissez l'opération que vous souhaitez effectuer :

- `RESET` : Réinitialise le quota pour une entrée spécifique dans le cache de quota du proxy.
- `SEARCH` : Liste de recherche des entrées d'utilisateur dans le cache de quota du proxy.
- `RESETALL` : Réinitialise toutes les entrées du cache des quotas de proxy.

Note Dans un mode multi-proxy, lorsque vous souhaitez réinitialiser l'appliance tout en accédant à *quotoquery* à partir de l'interface de ligne de commande, si le nom d'utilisateur du quota se compose d'un caractère « \ », ajoutez un autre « \ », puis réinitialisez l'appliance. Par exemple, si vous trouvez un nom d'utilisateur de quota « vol:W2012-01\administrator@AD1 », avant d'effectuer une réinitialisation, modifiez-le (ajoutez « \ ») comme suit : « W2012-01\\administrator@AD1 ». Le préfixe « vol: » n'est pas requis lorsque vous effectuez une réinitialisation.

reboot (redémarrer)

Vide le cache du système de fichiers sur le disque, arrête tous les processus en cours et redémarre le système.

reportingconfig

configurer un système de rapports.

resetconfig

Rétablit les valeurs par défaut de la configuration.

revert

Rétablit une version précédente qualifiée du système d'exploitation AsyncOS pour le Web. Il s'agit d'une action très destructrice, car elle détruit tous les journaux de configuration et bases de données. Reportez-vous à Retour à une version antérieure d'AsyncOS pour le Web, on page 621 pour en savoir plus sur l'utilisation de cette commande.

rollbackconfig

Vous permet de restaurer l'une des 10 configurations validées précédemment. Par défaut, la fonctionnalité de configuration de restauration est activée.

rollovernow

Renouvelle un fichier journal.

routeconfig

Configure les adresses IP de destination et les passerelles pour le trafic. Affiche les routages actuellement configurés et fournit un menu des opérations pour créer, modifier, supprimer ou effacer des entrées.

saveconfig

Enregistre une copie des paramètres de configuration actuels dans un fichier. Ce fichier peut être utilisé pour restaurer les paramètres par défaut, au besoin.

Si le mode FIPS est activé, fournissez une option de gestion de la phrase secrète : `Mask passphrases` (Masquer les phrases secrètes) ou `Encrypt passphrases` (Chiffrer les phrases secrètes).

setgateway

Configure la passerelle par défaut pour l'appareil.

sethostname

Définit le paramètre de nom d'hôte.

setntlmsecuritymode

Modifie le paramètre de sécurité du domaine d'authentification NTLM pour « ads » ou « domain ».

- `domain` : AsyncOS joint le domaine Active Directory avec un compte d'approbation de sécurité de domaine. AsyncOS nécessite Active Directory pour utiliser uniquement les groupes Active Directory imbriqués dans ce mode.
- `ads` : AsyncOS rejoint le domaine en tant que membre Active Directory natif.

La valeur par défaut est `ads`.

settime

Règle l'heure du système.

settz

Affiche le fuseau horaire actuel et la version du fuseau horaire. Fournit un menu des opérations pour définir un fuseau horaire local.

showconfig

Affiche toutes les valeurs de configuration.

Note Les phrases secrètes des utilisateurs sont chiffrées.

shutdown

Met fin aux connexions et arrête le système.

smbprotoconfig

Active ou désactive la prise en charge du protocole SMB1 pour Samba version 4.11.15.

Choisissez l'opération que vous souhaitez effectuer :

- Enable (activer) : active le protocole SMB1.
- Disable (désactiver) : désactive le protocole SMB1.

smtprelay

Configure les hôtes de relais SMTP pour les courriels générés à l'interne. Un hôte de relais SMTP est nécessaire pour recevoir les courriels et les alertes générés par le système.

smtpconfig

Configure l'hôte local pour qu'il écoute les requêtes SNMP et autorise les requêtes SNMP.

sshconfig

Configure les options de nom d'hôte et de clé d'hôte pour les serveurs approuvés.

sslconfig

Le chiffrement par défaut pour AsyncOS versions 9.0 et antérieures est `Default:+kEDH`.

Le chiffrement par défaut pour les versions 9.1 à 11.8 d'AsyncOS est le suivant :

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

Dans ce cas, le chiffrement par défaut peut changer en fonction de vos sélections de chiffrement ECDHE.

Le chiffrement par défaut pour AsyncOS versions 12.0 et ultérieures est :

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

Note Mettez à jour la suite de chiffrement par défaut lors de la mise à niveau vers une version plus récente d'AsyncOS. Les suites de chiffrements ne sont pas automatiquement mises à jour. Lorsque vous effectuez une mise à niveau d'une version antérieure vers AsyncOS 12.0 ou une version ultérieure, Cisco recommande de mettre à jour la suite de chiffrement pour :

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

FALLBACK : active/désactive l'option de repli SSL/TLS. Si elle est activée, les communications avec les serveurs distants utiliseront le protocole configuré le plus bas à la suite d'un échec d'établissement de liaison.

Une fois qu'une version de protocole est négociée entre le client et le serveur, un échec de l'établissement de liaison est possible en raison de problèmes de mise en œuvre. Si cette option est activée, le proxy tente de se connecter en utilisant la version la plus basse des protocoles TLS/SSL actuellement configurés.

Note Sur les nouvelles installations d'AsyncOS 9.x, le repli est désactivé par défaut. Pour les mises à niveau de versions antérieures pour lesquelles l'option de secours existe, le paramètre actuel est conservé; Sinon, lors de la mise à niveau à partir d'une version pour laquelle l'option n'existe pas, le repli est activé par défaut.

ECDHE : active/désactive l'utilisation des chiffrements ECDHE pour LDAP.

Les chiffrements ECDH supplémentaires sont pris en charge dans les versions successives; cependant, certaines courbes nommées fournies avec certains des chiffrements supplémentaires amènent l'appliance à fermer la connexion pendant l'authentification LDAP sécurisée et le déchiffrement du trafic HTTPS. Consultez Configuration SSL , on page 606 pour plus d'informations sur la spécification de chiffrements supplémentaires.

Si vous rencontrez ces problèmes, utilisez cette option pour désactiver ou activer l'utilisation du chiffrement ECDHE pour l'une ou l'autre des fonctionnalités ou pour les deux.

ssltool

Exécute différentes commandes OpenSSL à partir de l'interface de ligne de commande de l'appliance pour dépanner les connexions SSL. La commande `ssltool` comprend les sous-commandes suivantes :

- **`sclient`** : il s'agit de la version d'interface de ligne de commande de la commande openssl s_client. Elle se connectera à un hôte distant à l'aide de SSL/TLS directement, sans utiliser l'appliance.
  - `COMMAND :` exécute une commande openssl s_client. Les commandes openssl s_client suivantes sont prises en charge :

    ```
    -connect, -servername, -verify, -cipher, -verify_return_error, -reconnect, -pause,
     -showcerts, -prexit, -state, -debug, -msg, -tls1, -tls1_1, -tls1_2, -no_ssl2,
    -no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2, -tlsextdebug, -no_ticket, -status,
    -save, -noout
    ```

    Consultez l'aide en ligne pour plus d'informations sur les commandes openssl s_client prises en charge.

Note Après avoir exécuté `command`, vous pouvez enregistrer le résultat dans un fichier à l'aide de l'option `-save`. Vous ne pouvez pas accéder aux fichiers journaux enregistrés. Ces fichiers journaux sont utilisés par l'équipe d'assistance de Cisco pour le débogage.

  - `HELP` : fournit des informations d'aide.

- **`CLEARLOGS`** : supprime tous les journaux générés par `ssltool`.

status

Affiche l'état du système.

supportrequest

Envoie le courriel de demande d'aide à l'assistance client de Cisco. Cela comprend les informations sur le système et une copie de la configuration principale.

(Facultatif) Si vous fournissez le numéro de la demande de service, un ensemble plus vaste d'informations sur le système et la configuration est automatiquement ajouté à la demande de service. Ces informations sont compressées et téléchargées vers la demande de service par FTP.

tail

Affiche la fin d'un fichier journal. La commande accepte le nom du fichier journal comme paramètre.

Exemple 1

```
example.com> tail
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
```

```
…
…
Enter the number of the log you wish to tail.
[]> 9
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 10:03:07 2017 Info: Begin Logfile
~
~
…
…
“CTRL-C” + “q”
```

Exemple 2

```
example.com> tail system_logs
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 09:59:10 2017 Info: Begin Logfile
…
…
“CTRL-C” + “q”
```

tcpservices

Affiche des informations sur les services TCP/IP ouverts.

techsupport

Fournit une connexion temporaire pour permettre à l’assistance client de Cisco d’accéder au système et d’aider au dépannage.

telnet

Communique avec un autre hôte à l’aide du protocole TELNET, généralement utilisé pour vérifier la connectivité.

testauthconfig

Teste les paramètres d’authentification pour un domaine d’authentification donné par rapport aux serveurs d’authentification définis dans le domaine.

testauthconfig [-d level] [nom du domaine]

L’exécution de la commande sans aucune option permet à l’appliance de répertorier les domaines d’authentification configurés parmi lesquels vous pouvez effectuer une sélection.

L’indicateur de débogage (`-d`) contrôle le niveau d’informations de débogage. Les niveaux peuvent varier entre 0 et 10. Si cela n’est pas spécifié, l’appliance utilise le niveau 0. Au niveau 0, la commande renverra une réussite ou un échec. Si les paramètres de test échouent, la commande répertorie la cause de l’échec.

Note Cisco vous recommande d’utiliser le niveau 0. N’utilisez un niveau de débogage différent que lorsque vous avez besoin d’informations plus détaillées pour le dépannage.

tuiconfig tuistatus

Ces deux commandes sont documentées dans Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur, on page 112.

traceroute (afficher route)

Permet de suivre les paquets IP dans les passerelles et le long du chemin jusqu'à un hôte de destination.

trailblazerconfig

Vous pouvez utiliser la commande `trailblazerconfig` pour acheminer vos connexions entrantes et sortantes par les ports HTTP et HTTPS de la nouvelle interface Web.

Note Par défaut, la commande dans l'interface de ligne de commande `trailblazer` est activée sur votre appliance. Vous pouvez consulter l'aide en ligne en saisissant la commande suivante : `hello config`.

La syntaxe est la suivante :

```
trailblazerconfig enable <https_port> <http_port>

trailblazerconfig disable

trailblazerconfig status
```

Lieu :

« `enable` » exécute la commande trailblazer sur les ports par défaut (HTTPS : 4431 ou HTTP : 801).

« `disable` » met fin à la commande trailblazer.

« `status` » vérifie l'état de la commande trailblazer.

Note Si vous avez activé la commande `trailblazerconfig` sur l'appliance, l'URL de la demande contiendra le numéro de port HTTP/HTTPS ajouté au nom d'hôte.

Vous pouvez essayer l'une ou l'autre des étapes suivantes pour faciliter la navigation dans votre navigateur :

- Acceptez le certificat utilisé par l'interface Web et utilisez la syntaxe d'URL suivante : `https://hostname:<https_api_port> (par exemple, https://un.exemple.com:6443)` dans une nouvelle fenêtre de navigateur et acceptez le certificat. Ici `<https_api_port>` est le port HTTPS de l'API AsyncOS configuré dans **Network > IP Interfaces**(Réseau > Interfaces IP). Assurez-vous également que les ports API (HTTP/HTTPS) sont ouverts sur le pare-feu.
- Par défaut, la commande dans l'interface de ligne de commande `trailblazer` est activée sur votre appliance. Assurez-vous que les ports HTTP/HTTPS sont ouverts sur le pare-feu. Assurez-vous également que votre serveur DNS est capable de résoudre le nom d'hôte que vous avez spécifié pour accéder à l'appliance.

  Si la commande d'interface de ligne de commande `trailblazerconfig` est désactivée, vous pouvez exécuter la commande, vous pouvez exécuter la commande **trailblazerconfig** > **enable** à l'aide de l'interface de ligne de commande pour éviter les problèmes suivants :

  - Nécessité d'ajouter plusieurs certificats pour les ports d'API dans certains navigateurs.

- Redirection vers l'interface Web existante lorsque vous actualisez la page de mise en quarantaine des pourriels, de liste des autorisations ou de liste de blocage.
- La barre des mesures sur la page de rapport Cisco Secure Endpoint ne contient aucune donnée.

updateconfig

Configure les paramètres de mise à jour et de mise à niveau.

updatenow

Met à jour tous les composants.

upgrade

Installe la mise à niveau logicielle du système d'exploitation asynchrone.

`downloadinstall` : télécharge et installe immédiatement un pack de mise à niveau.

`download` : télécharge et enregistre le pack de mise à niveau pour l'installer ultérieurement.

Après avoir saisi l'une de ces commandes, une liste des pack de mise à niveau applicables à ce Secure Web Appliance s'affiche. Sélectionnez le pack souhaité en saisissant son numéro d'entrée, puis en appuyant sur Entrée; le téléchargement commence en arrière-plan. Pendant le téléchargement, des sous-commandes supplémentaires sont disponibles : `downloadstatus` et `canceldownload`.

Une fois le téléchargement terminé, si vous avez initialement saisi `downloadinstall`, l'installation commence immédiatement. Si vous avez entré `download`, deux commandes supplémentaires sont disponibles une fois le téléchargement terminé : `install` et `delete`. Entrez `install` pour commencer l'installation d'un pack téléchargé précédemment. Utilisez `delete` pour supprimer le pack téléchargé précédemment depuis Secure Web Appliance.

userconfig

Configure les administrateurs système.

version

Affiche des informations générales sur le système, les versions installées du logiciel système et les définitions de règles.

wccpstat

`all` : affiche les détails de tous les groupes de services WCCP (Web Cache Communication Protocol).

`servicegroup` : affiche les détails d'un groupe de services WCCP spécifique.

webcache

Examine ou modifie le contenu du cache de proxy, ou configurez des domaines et des URL que l'appliance ne met jamais en cache. Permet à un administrateur de supprimer une URL particulière du cache proxy ou de spécifier les domaines ou les URL à ne jamais stocker dans le cache proxy.

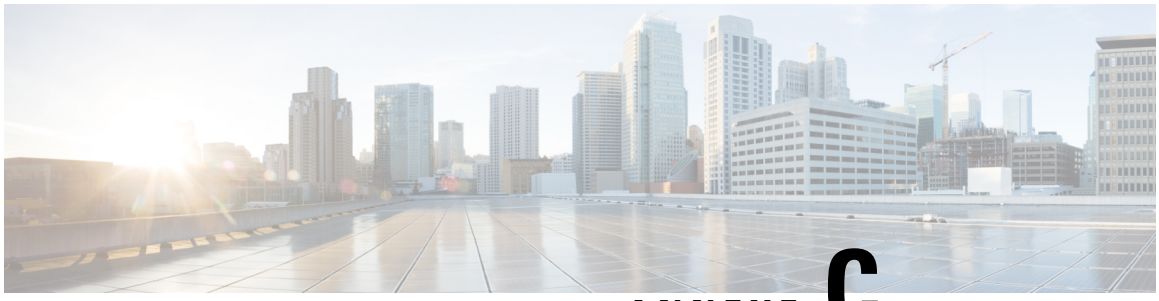
who

Affiche les utilisateurs connectés au système, pour les sessions d'interface de ligne de commande et Web.

Note Les utilisateurs individuels peuvent avoir un maximum de 10 sessions simultanées.

whoami

Affiche les informations concernant l'utilisateur.



ANNEXE C

Autres renseignements

Cette rubrique contient les sections suivantes :

Service de notification Cisco

Inscrivez-vous pour recevoir des notifications pertinentes pour vos appliances Cisco Content Security Appliances, comme des avis de sécurité, des avis de terrain, des déclarations de fin de vente et de prise en charge, ainsi que des informations sur les mises à jour logicielles et les problèmes connus.

Vous pouvez définir des options comme la fréquence des notifications et les types de renseignements à recevoir. Vous devez vous inscrire séparément aux notifications concernant chaque produit que vous utilisez.

Pour vous inscrire, visitez http://www.cisco.com/cisco/support/notifications.html

Un compte Cisco.com est requis. Si vous n'en avez pas, consultez Création d'un compte Cisco pour accéder aux ressources , on page 697.

Documentation

La documentation connexe concernant les Secure Web Appliance de Cisco est disponible aux emplacements suivants :

Produit	Lien
Secure Web Appliances (Comprend la documentation du matériel.)	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Produit	Lien
Appliances Content Security Management (Comprend la documentation du matériel.)	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Cloud Web Security (Comprend la documentation du matériel.)	http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

Formation

Formation sur les produits de sécurité pour la messagerie et le Web de Cisco :

http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html

Articles de la base de connaissances (TechNotes)

Étape 1 Accédez à la page principale sur le produit (http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html).

Étape 2 Recherchez les liens avec **TechNotes** dans le nom.

Communauté de soutien Cisco

Accédez à la communauté d'assistance Cisco pour la sécurité Web et la gestion associée à l'adresse URL suivante :

https://supportforums.cisco.com/community/5786/web-security

La communauté d'assistance Cisco est un lieu où discuter de questions générales portant sur la sécurité du Web et où obtenir des renseignements techniques sur des produits Cisco spécifiques. Par exemple, les messages peuvent inclure des vidéos de dépannage.

Service à la clientèle

Centre d'assistance technique Cisco (TAC) : http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Sites d'assistance pour l'ancien IronPort : http://www.cisco.com/web/services/acquisitions/ironport.html

Pour obtenir des instructions sur les appliances virtuelles, consultez le *Guide d'installation des appliances virtuelles de sécurité de contenu Cisco.*

Pour les problèmes non critiques, vous pouvez également ouvrir une demande d'assistance à partir de l'appliance.

Thèmes connexes

- Collaboration avec le service d'assistance , on page 663

Création d'un compte Cisco pour accéder aux ressources

L'accès à de nombreuses ressources sur Cisco.com nécessite un compte Cisco.

Si vous n'avez pas d'ID utilisateur Cisco.com, vous pouvez vous inscrire ici : https://tools.cisco.com/RPF/register/register.do

Cisco apprécie vos commentaires

L'équipe en charge des publications techniques de Cisco souhaite améliorer la documentation du produit. Vos commentaires et suggestions sont toujours les bienvenus. Vous pouvez envoyer vos commentaires à l'adresse de messagerie suivante : contentsecuritydocs@cisco.com

Veuillez préciser le titre de ce manuel et la date de publication indiquée sur la page de titre dans l'objet de votre message.

Contributeurs tiers

Certains logiciels inclus dans AsyncOS sont distribués selon les conditions, les avis et les conditions des contrats de licence de logiciels de FreeBSD, Inc., du Stichting Materials Centum, de la Corporation for National Research Initiatives, Inc. et d'autres contributeurs tiers, et toutes ces conditions générales sont intégrées dans les contrats de licence. Le texte intégral de ces ententes se trouve ici :

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

Des parties du logiciel dans AsyncOS sont basées sur l'outil RRD avec le consentement écrit exprès de Tobi Oeticker.

Des parties de ce document sont reproduites avec la permission de Dell Ordinateur Corporation. Des parties de ce document sont reproduites avec l'autorisation de McAfee, Inc. Des parties de ce document sont reproduites avec l'autorisation de Sophos Plc.

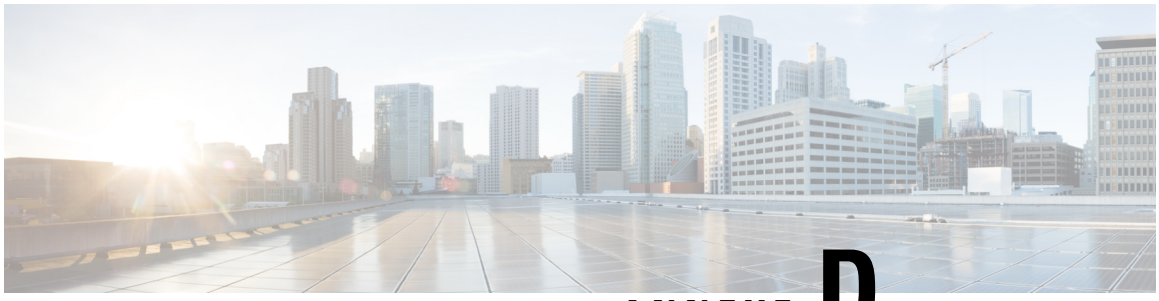
Gestion des renseignements permettant d'identifier une personne

Pour améliorer l'expérience de l'utilisateur et vous envoyer des notifications et des rapports en temps opportun, Cisco Secure Web Appliance recueille votre nom complet et votre adresse de messagerie.

L'appliance recueille ces informations lorsque l'administrateur crée des comptes utilisateur pour gérer Cisco Secure Web Appliance. Il est accessible uniquement au propriétaire du compte et à l'administrateur. Seul l'administrateur peut modifier ces informations.

Les informations sont stockées localement dans l'appliance et ne sont pas partagées avec des fonctions, des équipes ou des applications tierces.

Elles sont conservées jusqu'à ce que l'utilisateur dispose d'un compte Cisco Secure Web Appliance actif et sont supprimées du système lorsque l'administrateur supprime le compte d'utilisateur.



ANNEXE D

Contrat de licence de l'utilisateur final

Cette annexe contient les sections suivantes :

Contrat de licence de l'utilisateur final Cisco Systems

IMPORTANT : VEUILLEZ LIRE LE PRÉSENT CONTRAT DE LICENCE D'UTILISATEUR FINAL ATTENTIVEMENT. IL EST TRÈS IMPORTANT QUE VOUS VÉRIFIIEZ QUE VOUS ACHETEZ UN LOGICIEL OU UN ÉQUIPEMENT CISCO AUPRÈS D'UNE SOURCE APPROUVÉE ET QUE VOUS, OU L'ENTITÉ QUE VOUS REPRÉSENTEZ (COLLECTIVEMENT, LE « CLIENT ») AVEZ ÉTÉ ENREGISTRÉ EN TANT QU'UTILISATEUR FINAL AUX FINS DU PRÉSENT CONTRAT DE LICENCE UTILISATEUR FINAL DE CISCO. SI VOUS N'ÊTES PAS ENREGISTRÉ EN TANT QU'UTILISATEUR FINAL, VOUS N'AVEZ AUCUNE LICENCE D'UTILISATION DU LOGICIEL ET LA GARANTIE LIMITÉE DE CE CONTRAT DE LICENCE UTILISATEUR FINAL NE S'APPLIQUE PAS. EN SUPPOSANT QUE VOUS AYEZ ACHETÉ AUPRÈS D'UNE SOURCE APPROUVÉE, LE TÉLÉCHARGEMENT, L'INSTALLATION OU L'UTILISATION D'UN LOGICIEL CISCO OU FOURNI PAR CISCO CONSTITUE L'ACCEPTATION DU PRÉSENT CONTRAT.

CISCO SYSTEMS, INC. SA FILIALE CONCÉDANT LA LICENCE DU LOGICIEL AU LIEU DE CISCO SYSTEMS, INC. (« CISCO ») VOUS CONCÈDE LA LICENCE DE CE LOGICIEL UNIQUEMENT À LA CONDITION QUE VOUS AYEZ ACHETÉ LE LOGICIEL AUPRÈS D'UNE SOURCE APPROUVÉE ET QUE VOUS ACCEPTIEZ TOUTES LES CONDITIONS D'UTILISATION CONTENUES DANS CE CONTRAT DE LICENCE UTILISATEUR FINAL PLUS TOUTE LIMITATION SUPPLÉMENTAIRE À LA LICENCE ÉNONCÉE DANS UN CONTRAT DE LICENCE SUPPLÉMENTAIRE ACCOMPAGNANT LE PRODUIT OU DISPONIBLE AU MOMENT DE VOTRE COMMANDE (COLLECTIVEMENT LE « CONTRAT »). EN CAS DE CONFLITS ENTRE LES CONDITIONS DE CE CONTRAT DE LICENCE UTILISATEUR FINAL ET DE TOUT CONTRAT DE LICENCE SUPPLÉMENTAIRE, LE CONTRAT DE LICENCE SUPPLÉMENTAIRE S'APPLIQUERA. EN TÉLÉCHARGEANT, EN INSTALLANT OU EN UTILISANT LE LOGICIEL, VOUS RECONNAISSEZ AVOIR ACHETÉ LE LOGICIEL AUPRÈS D'UNE SOURCE APPROUVÉE ET VOUS ACCEPTEZ D'ÊTRE LIÉ PAR LE CONTRAT. SI VOUS N'ACCEPTEZ PAS L'ENSEMBLE DES CONDITIONS DU CONTRAT, CISCO NE VOUS CONCÉDERA PAS LA LICENCE DU LOGICIEL ET (A) VOUS NE POURREZ PAS TÉLÉCHARGER, INSTALLER OU UTILISER LE LOGICIEL ET (B) VOUS POURREZ RETOURNER LE LOGICIEL (Y COMPRIS LE CD NON OUVERT ET TOUT MATÉRIEL ÉCRIT) POUR UN REMBOURSEMENT COMPLET, OU, SI LE LOGICIEL ET LE MATÉRIEL ÉCRIT SONT FOURNIS DANS LE CADRE D'UN AUTRE PRODUIT,

Contrat de licence de l'utilisateur final

VOUS POURREZ RETOURNER L'ENSEMBLE DU PRODUIT POUR UN REMBOURSEMENT COMPLET. VOTRE DROIT DE RETOUR ET DE REMBOURSEMENT EXPIRE 30 JOURS APRÈS L'ACHAT AUPRÈS D'UNE SOURCE APPROUVÉE ET S'APPLIQUE UNIQUEMENT SI VOUS ÊTES L'ACHETEUR UTILISATEUR FINAL D'ORIGINE ET ENREGISTRÉ. AUX FINS DU PRÉSENT CONTRAT DE LICENCE UTILISATEUR FINAL, UNE « SOURCE APPROUVÉE » DÉSIGNE (A) CISCO; OU (B) UN DISTRIBUTEUR OU INTÉGRATEUR SYSTÈMES AUTORISÉ PAR CISCO À DISTRIBUER/VENDRE DES ÉQUIPEMENTS, LOGICIELS ET SERVICES CISCO SUR VOTRE TERRITOIRE AUX UTILISATEURS FINAUX; OU (C) UN REVENDEUR AUTORISÉ PAR UN TEL DISTRIBUTEUR OU INTÉGRATEUR SYSTÈMES CONFORMÉMENT AUX CONDITIONS DU CONTRAT DU DISTRIBUTEUR AVEC CISCO POUR DISTRIBUER/VENDRE LES ÉQUIPEMENT, LOGICIELS ET SERVICES CISCO SUR VOTRE TERRITOIRE AUX UTILISATEURS FINAUX.

LES CONDITIONS SUIVANTES DU CONTRAT RÉGISSENT L'UTILISATION DU LOGICIEL PAR LE CLIENT (DÉFINIE CI-DESSOUS), SAUF DANS LA MESURE OÙ : (A) IL EXISTE UN CONTRAT SIGNÉ SÉPARÉ ENTRE LE CLIENT ET CISCO RÉGISSANT L'UTILISATION DU LOGICIEL PAR LE CLIENT, OU (B) LE LOGICIEL COMPREND UN CONTRAT DE LICENCE DISTINCT SUIVANT LE PRINCIPE « D'ACCEPTATION PAR CLIC » OU UN CONTRAT DE LICENCE TIERS DANS LE CADRE DU PROCESSUS D'INSTALLATION OU DE TÉLÉCHARGEMENT RÉGISSANT L'UTILISATION DU LOGICIEL PAR LE CLIENT. EN CAS DE CONFLIT ENTRE LES CLAUSES DES DOCUMENTS PRÉCÉDENTS, L'ORDRE DE PRIORITÉ SERA (1) LE CONTRAT SIGNÉ, (2) LE CONTRAT SUIVANT LE PRINCIPE D'ACCEPTATION PAR CLIC OU LE CONTRAT DE LICENCE TIERS, ET (3) LE CONTRAT. AUX FINS DU CONTRAT, LE TERME « LOGICIEL » DÉSIGNE LES PROGRAMMES INFORMATIQUES, Y COMPRIS LES MICROLOGICIELS ET LES PROGRAMMES INFORMATIQUES INTÉGRÉS DANS L'ÉQUIPEMENT CISCO, TELS QUE FOURNIS AU CLIENT PAR UNE SOURCE APPROUVÉE, AINSI QUE TOUTES MISES À NIVEAU, MISES À JOUR, CORRECTIONS DE BOGUES OU VERSIONS MODIFIÉES DE CES VERSIONS (COLLECTIVEMENT, « MISE À NIVEAU »), TOUT ÉLÉMENT OBTENU DANS LE CADRE D'UNE RE-LICENCE EN VERTU DE LA POLITIQUE DE TRANSFERT ET DE RE-LICENCE DE LOGICIEL CISCO (TEL QU'ÉVENTUELLEMENT MODIFIÉ PAR CISCO DE TEMPS À AUTRE) OU DES COPIES DE SAUVEGARDE DE CE QUI PRÉCÈDE.

Licence. Sous réserve du respect des conditions du présent Contrat, Cisco accorde au Client une licence non exclusive et non cessible pour utiliser à des fins commerciales internes du Client le Logiciel et la Documentation pour lesquels le Client a payé les frais de licence requis à une Source approuvée. Le terme « Documentation » désigne les informations écrites (qu'elles soient contenues dans des manuels d'utilisation ou techniques, des supports de formation, des spécifications ou autre) relatives au Logiciel et mises à disposition par une Source approuvée avec le Logiciel de quelque manière que ce soit (notamment sur CD-Rom ou en ligne). Afin d'utiliser le Logiciel, le Client peut avoir à saisir un numéro d'enregistrement ou une clé d'autorisation de produit et à enregistrer une copie du Logiciel du Client en ligne sur le site Web de Cisco pour obtenir la clé ou le fichier de licence requis.

La licence du Client pour utiliser le Logiciel sera limitée, et le Client ne devra pas utiliser le Logiciel au-delà d'un seul châssis matériel ou d'une seule carte ou toute autre limitation énoncée dans le Contrat de Licence Supplémentaire applicable ou dans le bon de commande applicable qui a été accepté par une source approuvée et pour lequel le client a payé à une Source approuvée les frais de licence requis (le « bon de commande »).

Sauf disposition contraire expresse dans la Documentation ou dans tout Contrat de Licence Supplémentaire applicable, le Client doit utiliser le Logiciel uniquement tel qu'intégré, pour exécution sur ou (lorsque la Documentation applicable autorise l'installation sur un équipement non Cisco) pour la communication avec un équipement Cisco détenu ou loué par le Client et utilisé à des fins commerciales internes du Client. Aucune autre licence n'est accordée par implication, préclusion ou autrement.

Pour les copies d'évaluation ou les versions bêta pour lesquelles Cisco ne facture pas de frais de licence, l'obligation de payer les frais de licence décrite ci-dessus ne s'applique pas.

Restrictions générales Il s'agit d'une licence et non d'un transfert de propriété du Logiciel et de la Documentation, et Cisco conserve la propriété de toutes les copies du Logiciel et de la Documentation. Le Client reconnaît que le logiciel et la documentation contiennent des secrets commerciaux de Cisco, de ses fournisseurs ou de ses donneurs de licence, y compris, mais sans s'y limiter, la conception et la structure internes spécifiques de programmes individuels et d'informations sur l'interface associée. Sauf disposition expresse contraire du Contrat, le Client ne doit utiliser le Logiciel qu'en relation avec l'utilisation de l'équipement Cisco acheté par le Client auprès d'une Source approuvée et le Client n'a aucun droit, et le Client s'engage spécifiquement à ne pas :

(i) transférer, céder ou concéder en sous-licence ses droits de licence à toute autre personne ou entité (sauf en conformité avec toute politique de relicence/transfert de Cisco alors en vigueur), ou utiliser le logiciel sur un équipement Cisco non acheté par le client auprès d'une source approuvée ou sur du matériel Cisco d'occasion, et le Client reconnaît que toute tentative de transfert, de cession, de sous-licence ou d'utilisation sera nulle;

(ii) apporter des corrections d'erreurs ou autrement modifier ou adapter le Logiciel ou créer des œuvres dérivées basées sur le Logiciel, ou permettre à des tiers de faire de même;

(iii) faire de l'ingénierie inverse ou décompiler, déchiffrer, désassembler ou autrement réduire le Logiciel sous une forme lisible par l'homme, sauf dans la mesure expressément autorisée par la loi en vigueur nonobstant cette restriction ou sauf dans la mesure où Cisco est légalement tenu d'autoriser une telle activité spécifique conformément à toute licence open source applicable;

(iv) publier les résultats des tests de référence exécutés sur le Logiciel;

(v) utiliser ou permettre que le Logiciel soit utilisé pour fournir des services à des tiers, que ce soit sur la base d'un bureau de services, d'un temps partagé ou autre, sans l'autorisation écrite expresse de Cisco; ou

(vi) divulguer, fournir ou rendre disponible de toute autre manière les secrets commerciaux contenus dans le logiciel et la documentation sous quelque forme que ce soit à un tiers sans le consentement écrit préalable de Cisco. Le Client doit mettre en œuvre des mesures de sécurité raisonnables pour protéger ces secrets commerciaux.

Dans la mesure exigée par la loi en vigueur, et à la demande écrite du Client, Cisco fournira au Client les informations d'interface nécessaires pour assurer l'interopérabilité entre le Logiciel et un autre programme créé indépendamment, contre paiement des frais applicables de Cisco, le cas échéant. Le Client s'engage à respecter des obligations strictes de confidentialité à l'égard de ces informations et utilisera ces informations conformément aux conditions générales applicables selon lesquelles Cisco met ces informations à disposition.

Logiciels, mises à niveau et copies supplémentaires. NONOBSTANT TOUTE AUTRE DISPOSITION DU CONTRAT : (1) LE CLIENT N'A AUCUNE LICENCE NI DROIT DE RÉALISER OU D'UTILISER DES COPIES OU MISES À NIVEAU SUPPLÉMENTAIRES À MOINS QUE LE CLIENT, AU MOMENT DE LA RÉALISATION OU DE L'ACQUISITION DE CETTE COPIE OU MISE À NIVEAU, DÉTIENT DÉJÀ UNE LICENCE VALIDE POUR LE LOGICIEL ORIGINAL ET A PAYÉ LES FRAIS APPLICABLES À UNE SOURCE APPROUVÉE POUR LA MISE À NIVEAU OU LES COPIES SUPPLÉMENTAIRES; (2) L'UTILISATION DES MISES À NIVEAU EST LIMITÉE À L'ÉQUIPEMENT CISCO FOURNI PAR UNE SOURCE APPROUVÉE POUR LEQUEL LE CLIENT EST L'ACHETEUR FINAL OU LE LOCATAIRE INITIAL, OU DETIENT UNE LICENCE VALABLE D'UTILISATION DU LOGICIEL QUI EST EN COURS DE MISE À NIVEAU; ET (3) LA CRÉATION ET L'UTILISATION DE COPIES SUPPLÉMENTAIRES SONT LIMITÉES AUX FINS DE SAUVEGARDE NÉCESSAIRE SEULEMENT.

Avis de propriété intellectuelle. Le client s'engage à conserver et à reproduire tous les avis de droit d'auteur, de propriété et autres sur toutes les copies, sous quelque forme que ce soit, du Logiciel sous le même format et de la même manière que ces avis de droit d'auteur et autres avis de propriété sont inclus dans le Logiciel. Sauf autorisation expresse dans le Contrat, le Client ne doit effectuer aucune copie ou duplication d'un Logiciel sans l'autorisation écrite préalable de Cisco.

Durée et résiliation Le Contrat et la licence accordée dans les présentes demeurent en vigueur jusqu'à leur résiliation. Le Client peut résilier le Contrat et la licence à tout moment en détruisant toutes les copies du Logiciel et toute Documentation. Les droits du Client en vertu du Contrat prendront fin immédiatement sans préavis de Cisco si le Client ne respecte pas l'une des dispositions du Contrat. En cas de résiliation, le Client doit détruire toutes les copies du Logiciel et de la Documentation en sa possession ou sous son contrôle. Toutes les obligations de confidentialité du Client, toutes les restrictions et limitations imposées au Client en vertu de la section intitulée « Limitations générales » et toutes les limitations de responsabilité, exclusions de responsabilité et restrictions de garantie survivront à la résiliation du présent Contrat. En outre, les dispositions des articles intitulés « Acheteurs utilisateur final du gouvernement des États-Unis » et « Conditions générales applicables à la déclaration de garantie limitée et au Contrat de licence d'utilisateur final » survivent à la résiliation du Contrat.

Dossiers de clients. Le Client accorde à Cisco et à ses comptables indépendants le droit d'examiner les livres, registres et comptes du Client pendant les heures normales de bureau pour vérifier la conformité avec le présent Contrat. Dans le cas où un tel audit révèlerait un non-respect du présent Contrat, le Client devra rapidement payer à Cisco les frais de licence appropriés, ainsi que le coût raisonnable de la réalisation de l'audit.

Contrôles des exportations, des réexportations, des transferts et des utilisations. Le Logiciel, la Documentation et la technologie ou leurs produits directs (ci-après dénommés Logiciels et Technologie), fournis par Cisco dans le cadre du Contrat, sont soumis aux contrôles à l'exportation en vertu des lois et réglementations des États-Unis et de toutes les lois applicables des autres pays et règlements en vigueur. Le Client s'engage à respecter les lois et les règlements régissant l'exportation, la réexportation, le transfert et l'utilisation des Logiciels et Technologies Cisco et obtiendra toutes les autorisations, permis ou licences américains et locaux requis. Cisco et le Client acceptent chacun de fournir les autres informations, documents d'assistance et assistance qui peuvent raisonnablement être requis par l'autre dans le cadre de l'obtention d'autorisations ou de licences. Des renseignements concernant la conformité aux normes d'exportation, de réexportation, de transfert et d'utilisation se trouvent à l'adresse URL suivante :

https://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html

Acheteurs utilisateurs finaux du gouvernement des États-Unis. Le Logiciel et la Documentation sont des « articles commerciaux », tels que définis par la Réglementation des acquisitions fédérales (États-Unis, « FAR ») (48 C.F.R.) 2.101, et consistent en un « logiciel informatique commercial » et une « documentation logicielle commerciale », tels que désignés dans la réglementation FAR 12.212. Conforme à la norme FAR 12.212 et au sup. FAR du DoD. 227.7202-1 à 227.7202-4, et nonobstant toute autre réglementation FAR ou toute autre clause contractuelle contraire figurant dans un contrat pouvant intégrer le présent Contrat, le Client peut fournir à l'Utilisateur final du gouvernement ou, si le présent Contrat est direct, l'Utilisateur final du gouvernement pourra faire l'acquisition du Logiciel et de la Documentation avec seulement les droits mentionnés dans le présent Contrat. L'utilisation du Logiciel ou de la Documentation, ou des deux, implique l'acceptation, par le gouvernement, que le Logiciel et la Documentation sont un « logiciel informatique commercial » et une « documentation logicielle commerciale », et implique l'acceptation des droits et restrictions indiqués aux présentes.

Composants identifiés; Conditions supplémentaires Le Logiciel peut contenir ou être livré avec un ou plusieurs composants, qui peuvent inclure des composants tiers, identifiés par Cisco dans la Documentation, le fichier lisezmoi.txt, une acceptation par clic d'un tiers ou ailleurs (par exemple sur https://www.cisco.com/)) (le(s) « Composant(s) identifié(s) ») comme étant soumis à des conditions de contrat de licence, des exclusions de garantie, des garanties limitées ou d'autres conditions (collectivement, « Conditions supplémentaires ») différentes de celles énoncées dans les présentes. Vous acceptez les Conditions supplémentaires applicables pour ce(s) composant(s) identifié(s).

Garantie limitée

Sous réserve des limitations et conditions énoncées dans les présentes, Cisco garantit qu'à compter de la date d'expédition au client (mais en cas de revente par une source agréée autre que Cisco, à compter de quatre-vingt-dix (90) jours maximum après l'expédition initiale par Cisco), et se poursuivant pendant une période la plus longue entre (a) quatre-vingt-dix (90) jours ou (b) la période de garantie (le cas échéant) expressément énoncée comme applicable spécifiquement au logiciel dans la carte de garantie accompagnant le produit dont le Logiciel fait partie (le « Produit ») (le cas échéant) : (a) le support sur lequel le Logiciel est fourni est exempt de défauts de matériaux et de fabrication dans des conditions normales d'utilisation; et (b) le Logiciel est substantiellement conforme à la Documentation. La date d'expédition d'un produit par Cisco figure sur l'emballage dans lequel le produit est expédié. À l'exception de ce qui précède, le Logiciel est fourni « EN L'ÉTAT ». Cette garantie limitée s'étend uniquement au logiciel acheté auprès d'une source approuvée par un client qui est le premier utilisateur final enregistré. Le seul et unique recours du client et l'entière responsabilité de Cisco et de ses fournisseurs dans le cadre de cette garantie limitée seront (i) le remplacement du support défectueux et/ou (ii) à la discrétion de Cisco, la réparation, le remplacement ou le remboursement du prix d'achat du Logiciel, dans les deux cas, à la condition que toute erreur ou tout défaut constituant une violation de cette garantie limitée soit signalé à la Source approuvée fournissant le Logiciel au Client, pendant la période de garantie. Cisco ou la Source approuvée fournissant le logiciel au client peut, à sa discrétion, exiger le retour du logiciel et/ou de la documentation comme condition à l'application de la procédure. En aucun cas Cisco ne garantit que le Logiciel est exempt d'erreurs ou que le Client sera en mesure d'utiliser le Logiciel sans problèmes ni interruptions. De plus, en raison du développement continu de nouvelles techniques d'intrusion et d'attaque sur les réseaux, Cisco ne garantit pas que le logiciel ou tout équipement, système ou réseau sur lequel le logiciel est utilisé sera exempt de vulnérabilité à une intrusion ou à une attaque.

Restrictions. La présente garantie ne s'applique pas si le logiciel, le produit ou tout autre équipement sur lequel le logiciel est autorisé à être utilisé (a) a été modifié, sauf par Cisco ou son représentant autorisé, (b) n'a pas été installé, utilisé, réparé, ou entretenu conformément aux instructions fournies par Cisco, (c) a été soumis à des contraintes physiques ou électriques anormales, à des conditions environnementales anormales, à une mauvaise utilisation, à une négligence ou à un accident; ou (d) est sous licence à des fins bêta, d'évaluation, de test ou de démonstration. La garantie du Logiciel ne s'applique pas non plus à (e) des modules logiciels temporaires; (f) tout logiciel non publié sur le Centre de logiciels Cisco; (g) tout logiciel que Cisco fournit expressément « EN L'ÉTAT » sur le Centre de logiciels Cisco; (h) tout logiciel pour lequel une Source approuvée ne reçoit pas de frais de licence; et (i) des Logiciels fournis par un tiers qui n'est pas une Source approuvée.

EXONÉRATION DE GARANTIE

SAUF INDICATION CONTRAIRE DANS LA PRÉSENTE SECTION SUR LA GARANTIE, TOUTES LES CONDITIONS, LES DÉCLARATIONS ET LES GARANTIES EXPLICITES OU IMPLICITES, ENTRE AUTRES, TOUTE GARANTIE OU CONDITION IMPLICITE CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, L'ABSENCE DE CONTREFAÇON, LA QUALITÉ SATISFAISANTE, LA NON-INTERVENTION, L'EXACTITUDE DES RENSEIGNEMENTS OU DÉCOULANT D'UN COMPORTEMENT HABITUEL, DE LA LOI, DE L'USAGE OU DES PRATIQUES COMMERCIALES, SONT, PAR LA PRÉSENTE, EXCLUES DANS LA MESURE OÙ LA LOI EN VIGUEUR LE PERMET ET SONT EXPRESSÉMENT DÉCLINÉES PAR CISCO, SES FOURNISSEURS ET CONCÉDANTS. DANS LA MESURE OÙ L'EXCLUSION NE PEUT PAS ÊTRE EXCLUE, DE TELLES CONDITION, REPRÉSENTATION OU GARANTIE IMPLICITES SONT LIMITÉES À LA DURÉE DE LA GARANTIE EXPLICITE MENTIONNÉE DANS LA PARTIE « GARANTIE LIMITÉE » CI-DESSUS. ÉTANT DONNÉ QUE CERTAINS ÉTATS OU CERTAINES JURIDICTIONS N'AUTORISENT PAS LA LIMITATION DE LA DURÉE D'UNE GARANTIE IMPLICITE, LA RESTRICTION SUSMENTIONNÉE PEUT NE PAS S'APPLIQUER DANS CES ÉTATS. LA PRÉSENTE GARANTIE DONNE DES DROITS LÉGAUX SPÉCIFIQUES AU CLIENT, ET LE CLIENT PEUT ÉGALEMENT AVOIR D'AUTRES DROITS QUI VARIENT

D'UNE JURIDICTION À L'AUTRE. Les présentes clauses d'exonération et d'exclusion s'appliquent même si la garantie explicite susmentionnée ne répond pas à son objectif principal.

Exclusion de garantie et limitation de responsabilité. SI VOUS AVEZ ACQUIS LE LOGICIEL AUX ÉTATS-UNIS, EN AMÉRIQUE LATINE, AU CANADA, AU JAPON OU DANS LES CARAÏBES, NONOBSTANT TOUTE AUTRE DISPOSITION CONTRAIRE DU CONTRAT, TOUTE RESPONSABILITÉ DE CISCO, DE SES FILIALES, DIRIGEANTS, ADMINISTRATEURS, EMPLOYÉS, AGENTS, FOURNISSEURS ET CONCÉDANTS DE LICENCE COLLECTIVEMENT, AU CLIENT, QUE CE SOIT DANS LE CONTRAT, EN CAS DE DÉLIT (INCLUANT LA NÉGLIGENCE), DE VIOLATION DE LA GARANTIE OU AUTRE, NE DOIT PAS DÉPASSER LE PRIX PAYÉ PAR LE CLIENT À TOUTE SOURCE APPROUVÉE POUR LE LOGICIEL QUI A DONNÉ LIEU À LA RÉCLAMATION OU SI LE LOGICIEL FAIT PARTIE D'UN AUTRE PRODUIT, LE PRIX PAYÉ POUR CET AUTRE PRODUIT. La présente LIMITATION DE RESPONSABILITÉ POUR LE LOGICIEL EST CUMULATIVE ET NON PAR INCIDENT (C'EST-À-DIRE QUE L'EXISTENCE DE DEUX RÉCLAMATIONS OU PLUS N'ÉTENDRA PAS CETTE LIMITE).

SI VOUS AVEZ ACQUIS LE LOGICIEL EN EUROPE, AU MOYEN-ORIENT, EN AFRIQUE, EN ASIE OU OCÉANIE, NONOBSTANT TOUTE AUTRE DISPOSITION CONTRAIRE DU CONTRAT, TOUTE RESPONSABILITÉ DE CISCO, SES FILIALES, DIRIGEANTS, ADMINISTRATEURS, EMPLOYÉS, AGENTS, FOURNISSEURS ET CONCÉDANTS DE LICENCE COLLECTIVEMENT, POUR LE CLIENT, QUE CE SOIT AU CONTRAT, EN CAS DE DÉLIT (INCLUANT LA NÉGLIGENCE), DE VIOLATION DE LA GARANTIE OU AUTREMENT, NE DOIT PAS DÉPASSER LE PRIX PAYÉ À CISCO POUR LE LOGICIEL QUI DONNE LIEU À LA RÉCLAMATION OU SI LE LOGICIEL FAIT PARTIE D'UN AUTRE PRODUIT, LE PRIX PAYÉ POUR TEL AUTRE PRODUIT. La présente LIMITATION DE RESPONSABILITÉ POUR LE LOGICIEL EST CUMULATIVE ET NON PAR INCIDENT (C'EST-À-DIRE QUE L'EXISTENCE DE DEUX RÉCLAMATIONS OU PLUS N'ÉTENDRA PAS CETTE LIMITE). RIEN DANS CE CONTRAT NE LIMITE (I) LA RESPONSABILITÉ DE CISCO, DE SES SOCIÉTÉS AFFILIÉES, DIRIGEANTS, ADMINISTRATEURS, EMPLOYÉS, AGENTS, FOURNISSEURS ET CONCÉDANTS DE LICENCE AU CLIENT POUR BLESSURE OU DÉCÈS CAUSÉ PAR LEUR NEGLIGENCE, (II) LA RESPONSABILITÉ DE CISCO EN CAS DE FRAUDENTE (III) TOUTE RESPONSABILITÉ DE CISCO QUI NE PEUT ÊTRE EXCLUE EN VERTU DES LOIS APPLICABLES.

Avis de non-responsabilité – Renonciation de dommages indirects et autres pertes. SI VOUS AVEZ ACQUIS LE LOGICIEL AUX ÉTATS-UNIS, EN AMÉRIQUE LATINE, DANS LES CARAÏBES OU AU CANADA, QUE TOUT RECOURS ÉNONCÉ DANS LES PRÉSENTES ÉCHEC DE SON OBJECTIF ESSENTIEL OU AUTRE, EN AUCUN CAS CISCO OU SES FOURNISSEURS NE SERONT RESPONSABLES DE TOUTE PERTE DE REVENUS, DE BÉNÉFICES, OU PERTE OU ENDOMMAGEMENT DE DONNÉES, INTERRUPTION D'ACTIVITÉ, PERTE DE CAPITAL OU POUR DOMMAGES SPÉCIAUX, INDIRECTS, CONSÉCUTIFS, ACCESSOIRES OU PUNITIFS, QUELLE QU'EN SOIT LA CAUSE ET QUELLE QUE SOIT LA THÉORIE DE RESPONSABILITÉ OU QU'ILS DÉCOULENT DE L'UTILISATION OU DE L'INCAPACITÉ À UTILISER LE LOGICIEL OU AUTRE ET MÊME SI CISCO OU SES FOURNISSEURS OU CONCÉDANTS DE LICENCE ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES. DANS LA MESURE OÙ CERTAINS ÉTATS OU JURIDICTIONS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DES DOMMAGES CONSÉCUTIFS OU ACCESSOIRES, LA LIMITATION CI-DESSUS PEUT NE PAS S'APPLIQUER DANS VOTRE CAS.

SI VOUS AVEZ ACQUIS LE LOGICIEL AU JAPON, À L'EXCEPTION DE LA RESPONSABILITÉ DÉCOULANT DE OU EN RELATION AVEC UN DÉCÈS OU DES BLESSURES CORPORELLES, UNE FAUSSE DÉCLARATION FRAUDULEUSE, INDÉPENDAMMENT DE TOUT RECOURS ÉNONCÉ DANS LES PRÉSENTES QUI MANQUERAIT À SON OBJECTIF ESSENTIEL OU AUTRE, EN AUCUN CAS CISCO, SES FILIALES, DIRIGEANTS, ADMINISTRATEURS, EMPLOYÉS, AGENTS, FOURNISSEURS ET CONCÉDANTS DE LICENCE SONT RESPONSABLES DE TOUTE PERTE DE REVENUS, DE BÉNÉFICES OU DE DONNÉES PERDUES OU ENDOMMAGÉES, INTERRUPTION

D'ACTIVITÉ, PERTE DE CAPITAL OU DE DOMMAGES SPÉCIAUX, INDIRECTS, CONSÉCUTIFS, ACCESSOIRES OU PUNITIFS, QUELLE QU'EN SOIT LA CAUSE ET QUELLE QUE SOIT LA THÉORIE DE RESPONSABILITÉ OU QU'ELLE DÉCOULE DE L'UTILISATION OU DE L'INCAPACITÉ À UTILISER LE LOGICIEL OU AUTRE ET MÊME SI CISCO OU TOUTE SOURCE APPROUVÉE OU LEURS FOURNISSEURS OU CONCÉDANTS DE LICENCE ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES.

SI VOUS AVEZ ACQUIS LE LOGICIEL EN EUROPE, AU MOYEN-ORIENT, EN AFRIQUE, EN ASIE OU OCÉANIE, EN AUCUN CAS CISCO, SES FILIALES, DIRIGEANTS, ADMINISTRATEURS, EMPLOYÉS, AGENTS, FOURNISSEURS ET CONCÉDANTS DE LICENCE, NE SERONT RESPONSABLES DE TOUTE PERTE DE REVENUS, PERTE DE PROFIT OU PERTE DE DONNÉES OU DONNÉES ENDOMMAGÉES, INTERRUPTION D'ACTIVITÉS, PERTE DE CAPITAL OU POUR TOUS DOMMAGES SPÉCIAUX, INDIRECTS, CONSÉCUTIFS, ACCESSOIRES OU PUNITIFS, DE QUELQUE MANIÈRE QU'ILS DÉCOULENT, Y COMPRIS, SANS LIMITATION, D'UN CONTRAT, D'UN DÉLIT (Y COMPRIS LA NÉGLIGENCE) OU DE L'UTILISATION DE OU DE L'INCAPACITÉ D'UTILISER LE LOGICIEL, MÊME SI, DANS CHAQUE CAS, CISCO, SES FILIALES, DIRIGEANTS, ADMINISTRATEURS, EMPLOYÉS, AGENTS, FOURNISSEURS ET CONCÉDANTS DE LICENCE, ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES. DANS LA MESURE OÙ CERTAINS ÉTATS OU JURIDICTIONS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DES DOMMAGES CONSÉCUTIFS OU ACCESSOIRES, LA LIMITATION CI-DESSUS PEUT NE PAS S'APPLIQUER ENTIÈREMENT DANS VOTRE CAS. L'EXCLUSION CI-DESSUS NE S'APPLIQUE PAS À TOUTE RESPONSABILITÉ DÉCOULANT DE OU EN RELATION AVEC : (I) LE DÉCÈS OU DES BLESSURES CORPORELLES, (II) UNE FAUSSE DÉCLARATION FRAUDULEUSE OU (III) LA RESPONSABILITÉ DE CISCO EN RELATION AVEC TOUTES CONDITIONS QUI NE PEUVENT ÊTRE EXCLUES EN VERTU DE LA LOI APPLICABLE.

Le Client reconnaît et accepte que Cisco a fixé ses prix et conclu le Contrat en s'appuyant sur les exclusions de garantie et les limitations de responsabilité énoncées dans les présentes, et que ceux-ci reflètent une répartition des risques entre les parties (y compris le risque qu'un recours contractuel peut échouer à atteindre son objectif essentiel et entraîner des pertes consécutives), et que ceux-ci constituent une base essentielle du marché entre les parties.

Loi applicable, compétence juridictionnelle. Si vous avez acquis, en référence à l'adresse indiquée sur le bon de commande accepté par la source approuvée, le logiciel aux États-Unis, en Amérique latine ou dans les Caraïbes, le Contrat et les garanties (« Garanties ») sont contrôlés et interprétés conformément aux lois de l'État de Californie, États-Unis d'Amérique, nonobstant toute disposition relative aux conflits de lois; et les tribunaux d'État et fédéraux de Californie auront la compétence exclusive sur toute réclamation découlant du Contrat ou des Garanties. Si vous avez acquis le logiciel au Canada, sauf interdiction expresse de la loi locale, le Contrat et les garanties sont contrôlés et interprétés selon les lois de la province de l'Ontario, Canada, nonobstant tout conflit de dispositions légales; et les tribunaux de la province de l'Ontario auront la compétence exclusive sur toute réclamation découlant du Contrat ou des Garanties. Si vous avez acquis le Logiciel en Europe, au Moyen-Orient, en Afrique, en Asie ou en Océanie (à l'exclusion de l'Australie), sauf interdiction expresse par la loi locale, le Contrat et les Garanties sont contrôlés et interprétés selon les lois de l'Angleterre, nonobstant tout conflit de dispositions légales; et les tribunaux anglais auront la compétence exclusive sur toute réclamation découlant du Contrat ou des Garanties. En outre, si le Contrat est régi par les lois de l'Angleterre, aucune personne qui n'est pas partie au Contrat ne sera en droit d'appliquer ou de bénéficier de l'une de ses conditions en vertu de la loi de 1999 sur les contrats (droits des tiers). Si vous avez acquis le Logiciel au Japon, sauf interdiction expresse par la loi locale, le Contrat et les Garanties sont contrôlés et interprétés selon les lois du Japon, nonobstant tout conflit de dispositions légales; et le tribunal du district de Tokyo au Japon aura la compétence exclusive sur toute réclamation découlant du Contrat ou des garanties. Si vous avez acquis le logiciel en Australie, sauf interdiction expresse de la loi locale, le contrat et les garanties sont contrôlés et interprétés selon les lois de l'État de Nouvelle-Galles du Sud, en Australie, nonobstant tout conflit de dispositions légales; et les tribunaux d'État et fédéraux de la Nouvelle-Galles du Sud auront la

compétence exclusive sur toute réclamation découlant du Contrat ou des Garanties. Si vous avez acquis le Logiciel dans un autre pays, sauf interdiction expresse par la loi locale, le Contrat et les Garanties sont contrôlés et interprétés selon les lois de l'État de Californie, aux États-Unis d'Amérique, nonobstant tout conflit de dispositions légales; et les tribunaux d'État et fédéraux de Californie auront la compétence exclusive sur toute réclamation découlant du Contrat ou des Garanties.

Pour tous les pays visés ci-dessus, les parties déclinent spécifiquement l'application de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. Nonobstant ce qui précède, chaque partie peut demander une injonction provisoire auprès de tout tribunal compétent en ce qui concerne toute violation présumée de sa propriété intellectuelle ou de ses droits de propriété. Si une partie des présentes s'avère nulle ou inapplicable, les autres dispositions du Contrat et des garanties resteront pleinement en vigueur. Sauf disposition expresse des présentes, le Contrat constitue l'intégralité du contrat entre les parties en ce qui concerne la licence du Logiciel et de la Documentation et remplace toutes conditions contradictoires ou supplémentaires contenues dans tout Bon de Commande ou ailleurs, toutes conditions étant exclues. Le Contrat a été rédigé en langue anglaise et les parties conviennent que la version anglaise prévaudra.

Les conditions de la garantie et autres renseignements applicables aux produits Cisco peuvent être consultés à l'adresse suivante :

http://www.cisco.com/go/warranty

Contrat de licence d'utilisateur final supplémentaire pour les logiciels Cisco Systems Content Security

IMPORTANT : À LIRE ATTENTIVEMENT

Le présent contrat de licence d'utilisateur final supplémentaire (« CLUFS ») contient des conditions générales supplémentaires qui s'appliquent au produit logiciel visé par le contrat de licence d'utilisateur final (« CLUF ») convenu entre vous (dans les présentes, « vous » désigne vous et l'entité que vous représentez, aussi désignée par « Société ») et Cisco (collectivement, le « contrat »). Les termes commençant par une lettre majuscule utilisés dans ce CLUFS mais non définis dans la présente auront la signification qui leur a été donnée dans le CLUF. En cas de conflit entre les conditions générales du CLUF et celles du présent CLUFS, ces dernières prévaudront.

En plus des limitations indiquées dans le CLUF concernant votre accès et votre utilisation du Logiciel, vous acceptez de vous conformer à tout moment aux modalités et aux conditions indiquées dans ce CLUFS.

LE TÉLÉCHARGEMENT, L'INSTALLATION OU L'UTILISATION DU LOGICIEL CONSTITUE L'ACCEPTATION DU CONTRAT ET VOUS VOUS LIEZ, AINSI QUE L'ENTITÉ COMMERCIALE QUE VOUS REPRÉSENTEZ, AU CONTRAT. SI VOUS N'ACCEPTEZ PAS L'ENSEMBLE DES CONDITIONS DU CONTRAT, CISCO NE VOUS CONCÉDERA PAS LA LICENCE DU LOGICIEL ET (A) VOUS NE POURREZ PAS TÉLÉCHARGER, INSTALLER OU UTILISER LE LOGICIEL ET (B) VOUS POURREZ RETOURNER LE LOGICIEL (Y COMPRIS LE CD NON OUVERT ET TOUT MATÉRIEL ÉCRIT) POUR UN REMBOURSEMENT COMPLET, OU, SI LE LOGICIEL ET LE MATÉRIEL ÉCRIT SONT FOURNIS DANS LE CADRE D'UN AUTRE PRODUIT, VOUS POURREZ RETOURNER L'ENSEMBLE DU PRODUIT POUR UN REMBOURSEMENT COMPLET. LE LOGICIEL OU LE PRODUIT DOIT ÊTRE RETOURNÉ DANS LES 30 JOURS SUIVANT L'ACHAT AUPRÈS DE CISCO OU D'UN REVENDEUR AUTORISÉ POUR DONNER DROIT AU REMBOURSEMENT. SEUL L'ACHETEUR INITIAL PEUT BÉNÉFICIER DE CE DROIT.

Aux fins du présent CLUFS, le nom du produit et la description du produit que vous avez commandé sont l'une des appliances suivantes : Cisco Systems Email Security Appliance (« ESA »), Cisco Systems Secure

Web Appliance et Cisco Systems Security Management Application (« SMA ») (collectivement dénommées « Sécurité du contenu ») et leur appliance virtuelle équivalente (« Logiciel ») :

Cisco AsyncOS pour les courriels

Cisco AsyncOS pour le Web

Cisco AsyncOS pour la gestion

Antipourriel par courriel Cisco, antivirus Sophos

Cisco – Filtres antipropagation

Antipourriel Cloudmark

Cisco – Analyseur d'image

Antivirus McAfee

Cisco Intelligent Multi-Scan

Cisco Data Loss Prevention

Cisco – Chiffrement des courriels

Cisco – Mode d'envoi des courriels

Cisco – Contrôles d'utilisation du Web

Cisco – Réputation Web

Protection contre les programmes malveillants Sophos

Protection contre les programmes malveillants Webroot

McAfee Anti-Malware

Cisco – Signalement des courriels

Cisco – Suivi des courriels

Cisco – Quarantaine centralisée des courriels

Cisco – Signalement Web

Cisco – Politique Web et gestion de la configuration

Cisco – Gestion de la sécurité Web avancée avec Splunk

Chiffrement des courriels pour appareils de chiffrement

Chiffrement pour les courriels de masse générés par le système

Chiffrement des courriels et chiffrement à clé publique pour les appareils de chiffrement

Traitement de pièces jointes volumineuses pour les appareils de chiffrement

Licence de boîte courriel sécurisée pour les appareils de chiffrement

Définitions

Pour les besoins de ce SEULA, voici les définitions des termes clés utilisés :

Le terme « Service de la société » fait référence aux services de gestion des courriels, Internet et de sécurité fournis par la Société aux utilisateurs finaux dans le but de mener les activités commerciales internes de la Société.

Le terme « Utilisateur final » désigne : (1) pour Secure Web Appliance et SMA, l'employé, le sous-traitant ou un autre agent autorisé par la Société à accéder à Internet et à SMA par l'intermédiaire du Service de la Société ; et (2) pour ESA, les boîtes de courriel des employés, des sous-traitants ou d'autres agents autorisés par la Société à accéder aux services de courriel par le biais du service de la Société ou à les utiliser.

Le terme « Bon de commande » désigne le contrat d'achat, le contrat d'évaluation, le contrat de version bêta ou de précommercialisation ou tout autre contrat similaire conclu entre la Société et Cisco ou la Société et un revendeur Cisco, ou les modalités en vigueur de tout bon de commande accepté par Cisco en lien avec l'objet des présentes, renfermant les modalités d'achat s'appliquant à la licence du logiciel octroyée par le présent contrat.

« Information nominative » désigne tout renseignement qui peut être utilisé pour identifier une personne, y compris, mais sans s'y limiter, le nom d'une personne, son nom d'utilisateur, son adresse courriel et toute autre information nominative.

Le terme « Serveur » signifie un appareil ou un ordinateur physique lié à un réseau et qui gère les ressources du réseau ou qui approvisionne en ressources plusieurs utilisateurs.

« Services » désigne les services d'abonnement logiciel de Cisco.

Le terme « Description de service » signifie la description des Services d'Assistance à l'abonnement au Logiciel à https://www.cisco.com/c/en/us/about/legal/service-descriptions.html

Le terme « Données de télémesure » désigne des échantillons du trafic électronique et Web de la Société, notamment les données sur les attributs des courriels et des demandes Web ainsi que les renseignements sur la façon dont différents types de courriels et de demandes Web ont été traités par les produits matériels Cisco de la Société. Les métadonnées des messages électroniques et les demandes Web incluses dans les Données de télémesure sont anonymisées et obscurcies afin de supprimer toute information nominative.

« Durée » désigne la durée de l'abonnement logiciel que vous avez acheté, comme il est indiqué dans votre Bon de commande.

Le terme « Appliance virtuelle » désigne la version virtuelle des appliances de sécurité des courriels, Secure Web Appliance, et des appliances de gestion de la sécurité.

Le terme « Ordinateur virtuel » désigne un appareil logiciel pouvant exécuter son propre système d'exploitation et ses propres applications comme le fait un serveur.

Conditions générales supplémentaires sur la licence

OCTROIS DE LA LICENCE ET CONSENTEMENT AUX CONDITIONS DE COLLECTE DE DONNÉES

Licence du Logiciel.

En utilisant le Logiciel et la Documentation, la Société consent à être liée par les modalités du présent Contrat et, à condition que la Société soit en conformité avec le présent contrat, Cisco octroie à cette dernière une licence mondiale, non exclusive, incessible et ne pouvant faire l'objet d'une sous-licence pour l'utilisation du Logiciel pendant la durée de validité, et ce, uniquement sur les produits matériels Cisco, ou dans le cas des appliances virtuelles, sur une machine virtuelle, dans le cadre de la prestation de services de la Société aux utilisateurs finaux. Le nombre d'utilisateurs finaux autorisés à utiliser le logiciel est limité au nombre d'utilisateurs finaux spécifié dans les documents de commande. Dans le cas où le nombre d'utilisateurs finaux dans le cadre de la prestation des services par la Société dépasse le nombre d'utilisateurs finaux spécifié dans les documents de commande, la Société contactera une source approuvée pour acheter des licences logicielles supplémentaires. La durée de validité et l'étendue de cette licence sont définies plus précisément dans le Bon de commande. Le Bon de commande remplace le CLUF en ce qui concerne la durée de la licence du Logiciel. À l'exception des droits de licence expressément accordés, aucun droit, titre ou intérêt relatif à un quelconque logiciel n'est concédé à la Société par Cisco, par les revendeurs Cisco ou par leurs concédants de licence

respectifs. Votre droit aux mises à niveau du Logiciel est assujetti à la Description de service. Le présent Contrat et les services sont offerts conjointement.

Consentement et licence d'utilisation des données.

Conformément à la Déclaration de confidentialité de Cisco à l'adresse https://www.cisco.com/c/en/us/about/legal/privacy.html, la Société consent et accorde à Cisco, par la présente, une licence l'autorisant à recueillir et à utiliser les données de télémesure provenant de la Société. Cisco ne recueille ni n'utilise d'Information nominative dans les Données de télémesure. Cisco peut communiquer les Données de télémesure regroupées et anonymes à des tiers pour améliorer votre expérience de l'utilisateur, le Logiciel ainsi que d'autres produits et services de sécurité de Cisco. La Société peut résilier le droit de Cisco de recueillir les Données de télémesure à tout moment en désactivant la participation au réseau SenderBase dans le Logiciel. Les instructions à suivre pour activer ou désactiver la participation au réseau SenderBase sont accessibles dans le guide de configuration du Logiciel.

Descriptions des droits et obligations supplémentaires

Veuillez consulter le Contrat de licence d'utilisateur final de Cisco Systems, Inc., la Déclaration de confidentialité et la Description de service pour les Services d'Assistance aux Abonnements logiciels.

Contrat de licence de l'utilisateur final

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.