Règles de déchiffrement

Les rubriques suivantes fournissent une présentation de la création, de la configuration, de la gestion et du dépannage des règles de déchiffrement :

Remarque Comme TLS et SSL sont souvent utilisés de manière interchangeable, nous utilisons l'expression *TLS/SSL* pour indiquer que l'un ou l'autre des protocoles est l'objet de la discussion. Le protocole SSL a été déconseillé par l'IETF au profit du protocole TLS plus sécurisé. Vous pouvez donc interpréter le protocole *TLS/SSL* comme faisant uniquement référence à TLS.

Pour en savoir plus sur les protocoles SSL et TLS, consultez une ressource comme SSL ou TLS - What's the Difference?

Aperçu de Régles de déchiffrement

Les *Règles de déchiffrement* fournissent une méthode fine de gestion du trafic chiffré sur plusieurs périphériques gérés, qu'il s'agisse de bloquer le trafic sans autre inspection, de ne pas déchiffrer le trafic et de l'inspecter avec le contrôle d'accès, ou de déchiffrer le trafic pour une analyse de contrôle d'accès.

Exigences et conditions préalables pour les Régles de déchiffrement

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices et limites relatives à Règle de déchiffrement

Gardez les points suivants à l'esprit lors de la configuration de votre règles de déchiffrement. Configurer règles de déchiffrement correctement est une tâche complexe, mais essentielle à la création d'un déploiement efficace qui gère le trafic chiffré. De nombreux facteurs influencent la façon dont vous configurez les règles, y compris le comportement de certains applications que vous ne pouvez pas contrôler.

En outre, les règles peuvent se préempter, nécessiter des licences supplémentaires ou contenir des configurations non valides. Des règles bien configurées peuvent également réduire les ressources requises pour traiter le trafic réseau. La création de règles trop complexes et le mauvais classement des règles peuvent nuire aux performances.

Pour de plus amples renseignements, voir Bonnes pratiques pour les règles de contrôle d'accès.

Pour obtenir des consignes relatives spécifiquement à Accélération cryptographique TLS, consultez Accélération du chiffrement TLS.

Sujets connexes

Directives pour l'utilisation du déchiffrement TLS/SSL

Directives générales

Configurez les règles **Déchiffrement – Resigner** ou **Déchiffrer – Clé connue** *uniquement* si votre appareil géré gère le trafic chiffré. Régles de déchiffrement nécessitent une surcharge de traitement qui peut avoir un impact sur les performances.

Vous ne pouvez pas déchiffrer le trafic sur un périphérique doté d'interfaces en mode Tap passif ou en ligne.

Directives pour le trafic déchiffrable

Nous pouvons déterminer qu'une partie du trafic n'est pas déchiffrable, soit parce que le site Web lui-même n'est pas déchiffrable, soit parce que le site Web utilise l'épinglage SSL, qui empêche les utilisateurs d'accéder à un site déchiffré sans erreur dans leur navigateur.

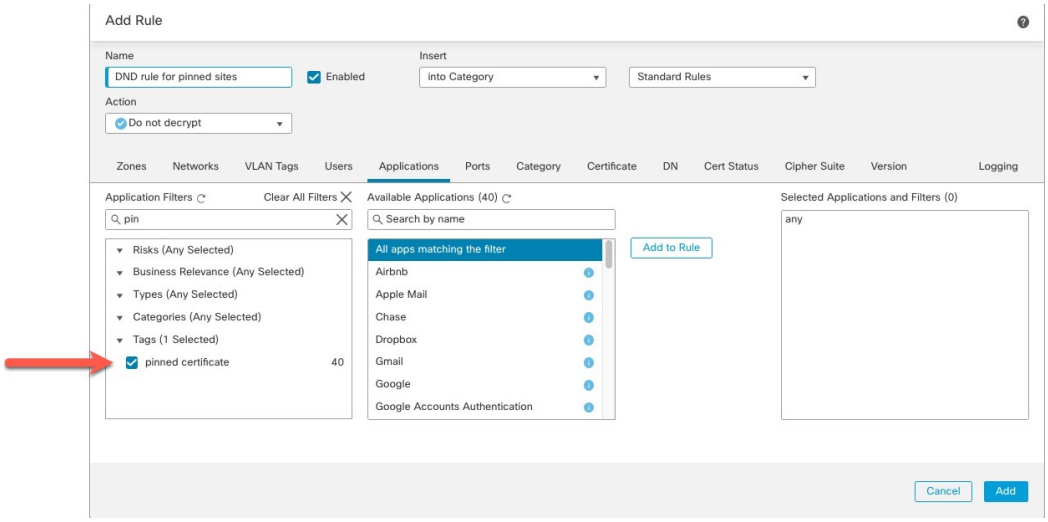
Pour en savoir plus sur l'épinglage de certificats, consultez À propos de l'épinglage TLS/SSL.

Nous maintenons la liste de ces sites comme suit :

- Un groupe de nom distinctif (DN) nommé **Cisco-Undecryptable-Sites**
- Le filtre d'application **certificat épinglé**

Si vous déchiffrez du trafic et que vous ne souhaitez pas que les utilisateurs voient des erreurs dans leur navigateur lorsqu'ils consultent ces sites, nous vous recommandons de configurer une règle « **Ne pas déchiffrer** » vers le bas de votre règles de déchiffrement.

Vous trouverez ci-dessous un exemple de configuration d'un filtre d'application de **certificat épinglé**.



Fonctionnalités Règle de déchiffrement non prises en charge

La suite de chiffrement CR4 n'est pas prise en charge

La suite de chiffrement Rivest Cipher 4 (également appelée *RC4* ou *ARC4*) est connue pour avoir des vulnérabilités et est considérée comme non sécurisée. Politiques de déchiffrement identifie la suite de chiffrement RC4 comme non prise en charge; vous devez configurer l'action **Unsupported Cipher Suite** (Suite de chiffrement non prise en charge) dans la page **Undecryptable Actions** (Actions indéchiffrables) de la politique selon les besoins de votre entreprise. Pour en savoir plus, consultez Options de traitement par défaut du trafic non déchiffrable.

Interfaces passives, en mode Tap en ligne et SPAN non prises en charge

Le trafic TLS/SSL ne peut pas être déchiffré sur les interfaces passives, en mode TAP en ligne ou SPAN.

Directives Ne pas déchiffrer TLS/SSL

Vous ne devez pas déchiffrer le trafic si cela est interdit par :

- la loi; Par exemple, certaines juridictions interdisent le déchiffrement des renseignements financiers
- la politique de l'entreprise; Par exemple, votre entreprise pourrait interdire le déchiffrement des communications privilégiées
- Règles de confidentialité
- Le trafic qui utilise l'épinglage de certificat (également appelé *TLS/SSL épinglage*) doit rester chiffré pour éviter de rompre la connexion

Le trafic chiffré peut être autorisé ou bloqué dans n'importe quelle condition règle de déchiffrement, y compris, mais sans s'y limiter :

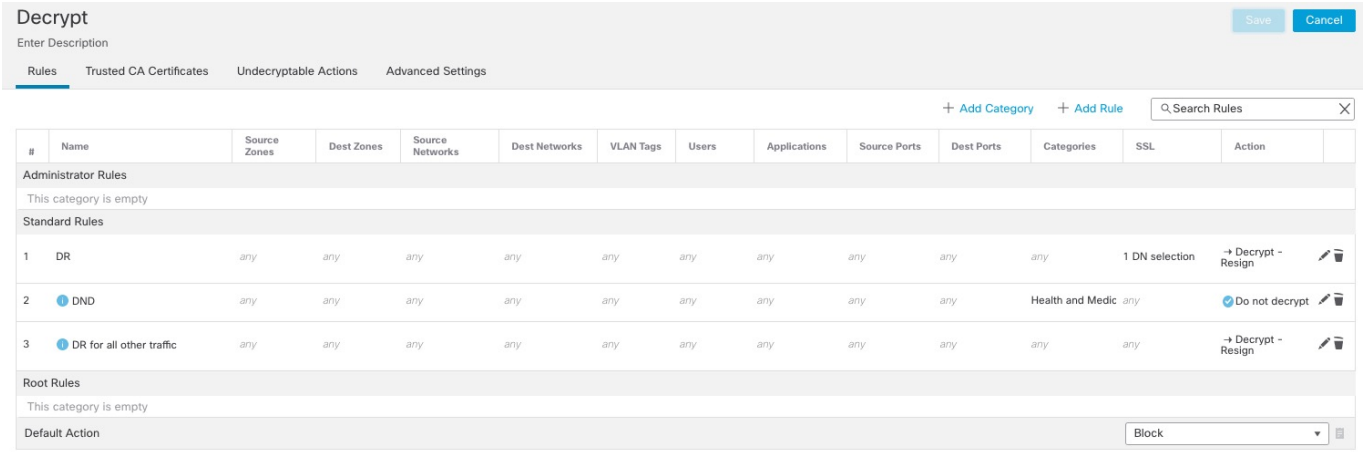
- État du certificat (par exemple, certificat expiré ou non valide)
- Protocole (par exemple, le protocole SSL non sécurisé)
- Réseau (zone de sécurité, adresse IP, balise VLAN, etc.)
- URL ou catégorie d'URL exacte
- Port
- Groupe d'utilisateurs

Limites des catégories dans les règles Ne pas déchiffrer

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise. Bien que nous nous efforcions de mettre à jour et d'améliorer continuellement les catégories de filtrage d'URL, ce n'est pas une science exacte. Certains sites Web ne sont pas du tout classés et il est possible que certains sites Web soient mal classés.

éviter d'utiliser trop de catégories dans les règles « ne pas déchiffrer » pour éviter le déchiffrement du trafic sans raison; Par exemple, la catégorie Santé et Médecine comprend le site Web WebMD, qui ne menace pas la vie privée des patientes.

Vous trouverez ci-dessous un exemple de politique de déchiffrement qui peut empêcher le déchiffrement des sites Web de la catégorie Santé et Médecine, mais autoriser le déchiffrement pour WebMD et tout le reste. Vous trouverez des renseignements généraux sur les règles de déchiffrement dans Directives pour l'utilisation du déchiffrement TLS/SSL, à la page 2.



Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications.

Directives Déchiffrer - Resigner de TLS/SSL

Vous pouvez associer un certificat d'autorité de certification (CA) interne et une clé privée à l'action **Déchiffrer – Resigner**. Si le trafic correspond à cette règle, le système signe de nouveau le certificat du serveur avec le certificat de l'autorité de certification, puis agit comme un intermédiaire. Cela crée deux sessions TLS/SSL, une entre le client et le périphérique géré, et une entre le périphérique géré et le serveur. Chaque session contient des détails de session cryptographiques différents et permet au système de déchiffrer et de rechiffrer le trafic.

Bonnes pratiques

Nous vous recommandons ce qui suit :

- Utilisez l'action de règle **Déchiffrer - Resigner** pour déchiffrer le trafic *sortant*, par opposition au trafic entrant pour lequel nous vous recommandons l'action de règle **Déchiffrer - Clé connue**.

  Pour plus d'informations sur **Déchiffrer - Clé connue** consultez Lignes directrices pour l'action déchiffrer - Clés connues TLS/SSL, à la page 7.

- Toujours cochez la case **Replace Key Only** (remplacement de la clé uniquement) lorsque vous configurez une action de règle **Decrypt - Resign (déchiffrer - resigner)**.

  Lorsqu'un utilisateur navigue sur un site Web qui utilise un certificat *autosigné*, il voit un avertissement de sécurité dans le navigateur Web et sait qu'il communique avec un site non sécurisé.

  Lorsqu'un utilisateur navigue sur un site Web qui utilise un certificat de confiance, il ne voit pas d'avertissement de sécurité.

Détails

Si vous configurez une règle avec l'action **Déchiffrer - Resigner**, la règle correspond au trafic en fonction du type d'algorithme de signature du certificat interne de l'autorité de certification référencé, en plus des conditions de la règle configurée. Comme vous associez un certificat d'autorité de certification à une action **Déchiffrer - Resigner**, vous ne pouvez pas créer un règle de déchiffrement qui déchiffre plusieurs types de trafic sortant chiffrés avec différents algorithmes de signature. En outre, tous les objets de certificat externe et les suites de chiffrement que vous ajoutez à la règle doivent correspondre au type d'algorithme de chiffrement du certificat d'autorité de certification associé.

Par exemple, le trafic sortant chiffré avec un algorithme de courbe elliptique (EC) correspond à une règle **Déchiffrer - Resigner** uniquement si l'action fait référence à un certificat basé sur une autorité de certification EC; vous devez ajouter des certificats externes basés sur EC et des suites de chiffrement à la règle pour créer des conditions de règles de certificat et de suite de chiffrement.

De même, une règle **Déchiffrer - Resigner** qui fait référence à un certificat d'autorité de certification basé sur RSA correspond uniquement au trafic sortant chiffré avec un algorithme RSA; le trafic sortant chiffré avec un algorithme EC ne correspond pas à la règle, même si toutes les autres conditions de règle configurées correspondent.

Directives et limites

Notez également les éléments suivants :

Suite de chiffrement anonyme non prise en charge

Par nature, les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification et n'utilisent pas les échanges de clés. Les utilisations des suites de chiffrement anonymes sont limitées; pour en savoir plus, consultez l'annexe F.1.1.1 de RFC 5246. (Remplacement de TLS 1.3 par l'annexe C.5 de la RFC 8446.)

Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification.

Action de la règle Déchiffrer - Resigner et une requête de signature de certificat (CSR)

Pour utiliser une action de règle **Déchiffrer – Resigner**, vous devez créer une requête de signature de certificat (CSR) et la faire signer par une autorité de certification de confiance. (Vous pouvez utiliser la console FMC pour créer une requête de signature de certificat (CSR) : **Objets** > **Gestion des objets** > **PKI** > **Autorités de certification internes**.)

Pour être utilisé dans une règle **Déchiffrement – Resigner**, l'autorité de certification (CA) doit avoir au moins l'une des extensions suivantes :

- **CA: TRUE**

  Pour en savoir plus, consultez l'examen des contraintes de base de la RFC 3280, section 4.2.1.10.

- **KeyUsage=CertSign**

  Pour obtenir de plus amples renseignements, consultez RFC 5280, section 4.2.1.3.

Pour vérifier que votre CSR ou votre autorité de certification possède au moins l'une des extensions précédentes, vous pouvez utiliser la commande **openssl**, comme indiqué dans une référence telle que la documentation openssl.

Cela est nécessaire, car pour que l'inspection de **déchiffrement - resigner** fonctionne, le certificat utilisé dans politique de déchiffrement génère des certificats à la volée et les signe pour agir comme intermédiaire et mandataire pour toutes les connexions TLS/SSL.

Épinglage de certificats

Si le navigateur du client utilise l'épinglage de certificat pour vérifier un certificat de serveur, vous ne pouvez pas déchiffrer ce trafic en signant de nouveau le certificat de serveur. Pour autoriser ce trafic, configurez un règle de déchiffrement avec l'action **Ne pas déchiffrer** pour qu'il corresponde au nom commun ou au nom unique du certificat de serveur.

Suite de chiffrement non correspondante

L'erreur suivante s'affiche si vous tentez d'enregistrer un règle de déchiffrement avec une suite de chiffrement qui ne correspond pas au certificat.

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

Autorité de certification non approuvée

Si le client ne fait pas confiance à l'autorité de certification (CA) utilisée pour signer de nouveau le certificat du serveur, le système avertit l'utilisateur que le certificat ne doit pas être approuvé. Pour éviter cela, importez le certificat d'autorité de certification dans le magasin d'autorités de certification de confiance du client. Sinon, si votre entreprise dispose d'une PKI privée, vous pouvez émettre un certificat d'autorité de certification intermédiaire signé par l'autorité de certification racine et qui est automatiquement approuvé par tous les clients de l'organisation, puis téléverser ce certificat d'autorité de certification sur le périphérique.

Limitation du serveur mandataire HTTP

Le système ne peut pas déchiffrer le trafic si un serveur mandataire HTTP est placé entre un client et votre périphérique géré, et si le client et le serveur établissent une connexion tunnel TLS/SSL à l'aide de la méthode HTTP CONNECT. L'action **Handshake Errors** (Erreurs d'établissement de liaison) non déchiffrables détermine la manière dont le système traite ce trafic.

Téléverser le certificat d'autorité de certification signé

Si vous créez un objet d'autorité de certification interne et que vous choisissez de générer une requête de signature de certificat (CSR), vous ne pouvez pas utiliser cette autorité de certification pour une action **Déchiffrer - Resigner** tant que vous n'avez pas téléversé le certificat signé sur l'objet.

Algorithme de signature non concordant

Si vous configurez une règle avec l'action **Déchiffrer - Resigner** et que le type d'algorithme de signature ne correspond pas à un ou plusieurs objets de certificat externe ou suites de chiffrement, l'éditeur de politique affiche un **Information** () à côté de la règle. Si vous ne correspondez pas au type d'algorithme de signature pour tous les objets de certificat externe ou toutes les suites de chiffrement, la politique affiche une icône d'avertissement **Avertissement** () à côté de la règle et vous ne pouvez pas déployer la politique de contrôle d'accès associée à politique de déchiffrement.

Lignes directrices pour l'action déchiffrer - Clés connues TLS/SSL

Lorsque vous configurez l'action **Déchiffrer - Clé connue**, vous pouvez associer un ou plusieurs certificats de serveur et des clés privées jumelées à l'action. Si le trafic correspond à la règle et que le certificat utilisé pour chiffrer le trafic correspond au certificat associé à l'action, le système utilise la clé privée appropriée pour obtenir les clés de chiffrement et de déchiffrement de la session. Comme vous devez avoir accès à la clé

privée, cette action est la mieux adaptée pour déchiffrer le trafic entrant vers les serveurs contrôlés par votre organisation.

Notez également les éléments suivants :

Suite de chiffrement anonyme non prise en charge

Par nature, les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification et n'utilisent pas les échanges de clés. Les utilisations des suites de chiffrement anonymes sont limitées; pour en savoir plus, consultez l'annexe F.1.1.1 de RFC 5246. (Remplacement de TLS 1.3 par l'annexe C.5 de la RFC 8446.)

Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification.

Impossible de trouver une correspondance sur le nom distinctif ou le certificat

Vous ne pouvez pas mettre en correspondance les conditions de **nom distinctif** ou de **certificat** lors de la création d'un règle de déchiffrement avec une action **Déchiffrer - Clé connue**. L'hypothèse est que si cette règle correspond au trafic, le certificat, le nom distinctif du sujet et le nom distinctif de l'émetteur correspondent déjà au certificat associé à la règle.

Le certificat de l'algorithme de signature numérique à courbe elliptique (*ECDSA*) bloque le trafic
(Déchiffrement TLS 1.3 activé uniquement.) Si vous utilisez un certificat ECDSA avec une action de règle **Déchiffrer - Clé connue**, le trafic correspondant sera bloqué. Pour éviter cela, utilisez un certificat avec un autre type de certificat.

Directives de blocage TLS/SSL

Si le trafic déchiffré correspond à une règle de contrôle d'accès avec une action **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (blocage interactif avec réinitialisation), le système affiche une page de réponse personnalisable.

Si vous avez activé la journalisation dans votre règle, deux événements de connexion sont affichés (dans **Analysis** > **Events** > **Connections**) : un événement pour le blocage interactif et un autre événement pour indiquer si l'utilisateur a choisi ou non de continuer sur le site.

Sujets connexes

Configurer les pages de réponse HTTP

Directives relatives à l'épinglage de certificats TLS/SSL

Certaines applications ont recours à une technique appelée « *TLS/SSL épinglage* » ou « épinglage de *certificat* », qui intègre l'empreinte du certificat de serveur d'origine dans l'application elle-même. Par conséquent, si vous avez configuré un règle de déchiffrement avec une action **Déchiffrer - Resigner**, lorsque l'application reçoit un certificat résigné d'un périphérique géré, la validation échoue et la connexion est abandonnée.

Comme l'épinglage TLS/SSL est utilisé pour éviter les attaques de l'homme du milieu, il n'y a aucun moyen de l'éviter ou de le contourner. Vous avez les options suivantes :

- Créez une règle **Ne pas déchiffrer** pour les applications classées avant les règles **Déchiffrer – Resigner**.
- Demander aux utilisateurs d'accéder aux applications à l'aide d'un navigateur Web.

Pour en savoir plus sur l'ordre des règles, consultez Ordre des règles SSL.

Pour déterminer si les applications utilisent l'épinglage TLS/SSL, consultez Dépanner l'épinglage TLS/SSL.

Directives de pulsation TLS/SSL

Certaines applications utilisent l'extension de *pulsation TLS* pour les protocoles Transport Layer Security (TLS) et DTLS (Datagram Transport Layer Security) définis par la RFC6520. La pulsation TLS permet de confirmer que la connexion est toujours active : le client ou le serveur envoie un nombre spécifié d'octets de données et demande à l'autre partie de renvoyer la réponse. Si l'opération réussit, des données chiffrées sont envoyées.

Vous pouvez configurer la **Max Heartbeat Length** (longueur de pulsation maximale) dans une politique d'analyse de réseau (Politique d'analyse de réseau (NAP)) pour déterminer comment gérer les pulsations TLS. Pour obtenir plus de renseignements, consultez Le préprocesseur SSL.

Pour en savoir plus, consultez À propos de TLS heartbeat (pulsations TLS).

Limites relatives à la suite de chiffrement anonyme TLS/SSL

Par nature, les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification et n'utilisent pas les échanges de clés. Les utilisations des suites de chiffrement anonymes sont limitées; pour en savoir plus, consultez l'annexe F.1.1.1 de RFC 5246. (Remplacement de TLS 1.3 par l'annexe C.5 de la RFC 8446.)

Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification.

Vous pouvez ajouter une suite de chiffrement anonyme à la condition **Cipher Suite** dans un règle de déchiffrement, mais le système supprime automatiquement les suites de chiffrement anonymes pendant le traitement de ClientHello. Pour que le système utilise la règle, vous devez également configurer vos règles de déchiffrement dans un ordre qui empêche le traitement de ClientHello. Pour en savoir plus, consultez Ordre des règles SSL.

Directives du normalisateur TLS/SSL

Si vous activez l'option **Normalize Excess Payload** (normaliser la charge utile excessive) dans le préprocesseur de normalisation en ligne, lorsque le préprocesseur normalise le trafic déchiffré, il peut abandonner un paquet et le remplacer par un paquet découpé. Cela ne met pas fin à la session TLS/SSL. Si le trafic est autorisé, le paquet découpé est chiffré dans le cadre de la session TLS/SSL.

Autres directives relatives à une Règle de déchiffrement

Utilisateurs et groupes

Si vous ajoutez un groupe ou un utilisateur à une règle, puis modifiez vos paramètres de domaine pour exclure ce groupe ou cet utilisateur, la règle n'a aucun effet. (Il en va de même pour la désactivation du domaine.) Pour en savoir plus sur les domaines, consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.

Catégories dans règles de déchiffrement

Si votre politique de déchiffrement a une action **Déchiffrer - Resigner** mais que les sites Web ne sont pas déchiffrés, consultez la page **Catégorie** sur les règles associées à cette politique.

Dans certains cas, un site Web effectue une redirection vers un autre site à des fins d'authentification ou à d'autres fins, la catégorisation d'URL du site redirigé peut être différente de celle du site que vous essayez de déchiffrer. Par exemple, `gmail.com` (catégorie **des courriels sur le Web**) redirige vers `comptes.gmail.com` (catégorie **portails Internet**) pour authentification. Assurez-vous d'inclure toutes les catégories pertinentes dans la règle SSL.

Remarque Afin de traiter entièrement le trafic en fonction de la catégorie d'URL, vous devez également configurer le filtrage d'URL. Consultez le chapitre Filtrage d'URL.

Requête d'URL ne figurant pas dans la base de données locale

Si vous créez une règle **Déchiffrer - Resigner** et que les utilisateurs accèdent à un site Web dont la catégorie et la réputation ne figurent pas dans la base de données locale, les données pourraient ne pas être déchiffrées. Certains sites Web ne sont pas classés dans la base de données locale et, si ce n'est pas le cas, les données de ces sites Web ne sont pas déchiffrées par défaut.

Vous pouvez contrôler ce comportement avec le paramètre **Système > Intégration >Services infonuagiques**, et cochez la case **Interroger le nuage Cisco pour les URL inconnues**.

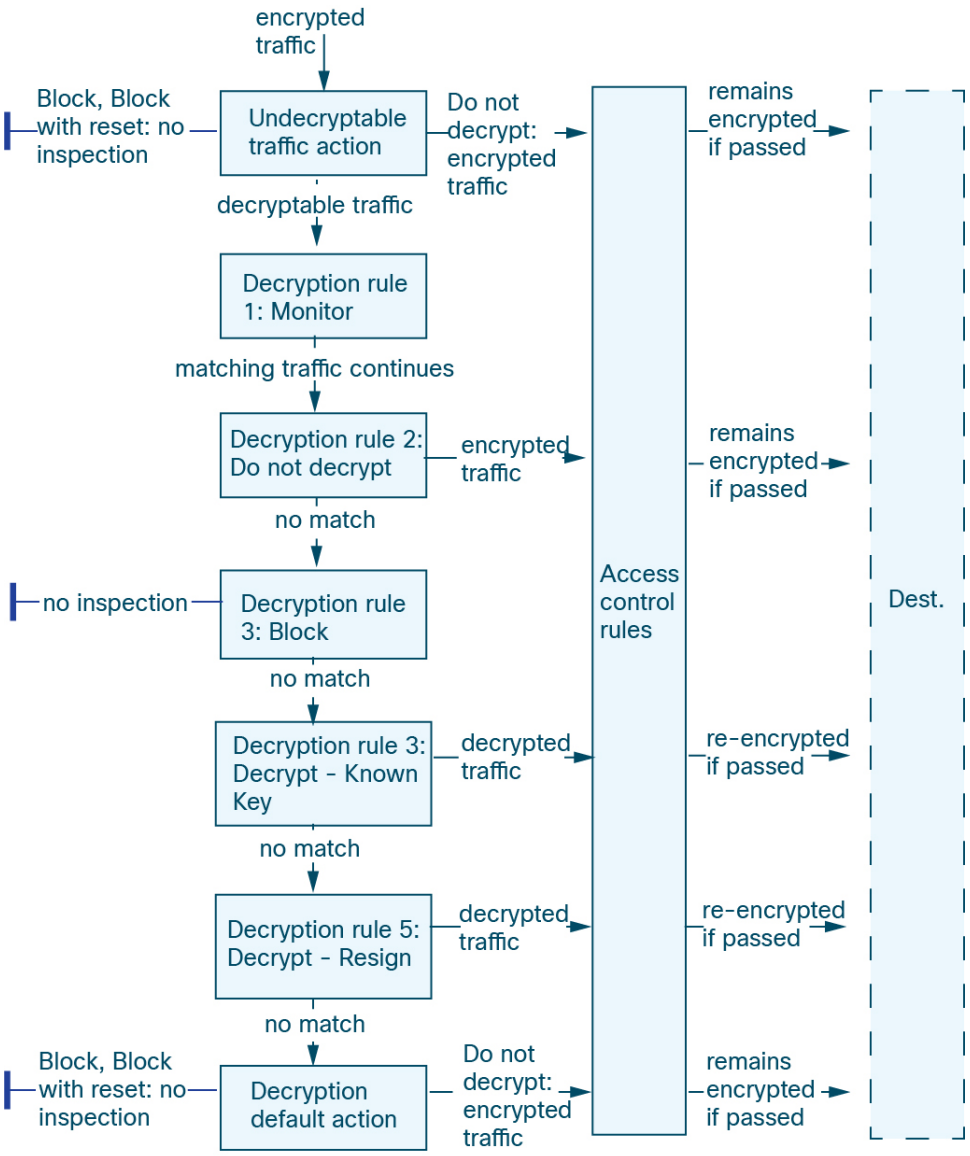
Pour en savoir plus sur cette option, consultez la section *Cisco Cloudsf* dans Guide d'administration Cisco Secure Firewall Management Center.

Gestion du trafic de Règle de déchiffrement

Le système fait correspondre le trafic vers règles de déchiffrement dans l'ordre que vous spécifiez. Dans la plupart des cas, le système gère le trafic chiffré en fonction du *premier* règle de déchiffrement cas, où *toutes* les conditions de la règle correspondent au trafic. Les conditions peuvent être simples ou complexes; vous pouvez contrôler le trafic par zone de sécurité, réseau ou emplacement géographique, VLAN, port, application, URL demandée, utilisateur, certificat, nom distinctif de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement.

Chaque règle possède également une *action*, qui détermine si vous surveillez, bloquez ou inspectez le trafic chiffré ou déchiffré correspondant à l'aide du contrôle d'accès. Vous observerez que le système n'inspecte *pas* davantage le trafic chiffré qu'il bloque. Il inspecte le trafic chiffré et non déchiffrable à l'aide du contrôle d'accès. Cependant, certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, de sorte que le trafic chiffré peut correspondre à moins de règles. En outre, par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées.

Le scénario suivant résume les façons dont règles de déchiffrement gère le trafic dans un déploiement en ligne.



Dans ce scénario, le trafic est évalué comme suit :

- **L'action Undecryptable Traffic** (Trafic non déchiffrable) évalue d'abord le trafic chiffré. En ce qui concerne le trafic que le système ne peut pas déchiffrer, il le bloque sans autre forme d'inspection ou le transmet à l'inspection du contrôle d'accès. Le trafic chiffré qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 1 : La règle Monitor (Surveiller)** évalue ensuite le trafic chiffré. Les règles de surveillance suivent et consignent le trafic chiffré, mais n'affectent pas le flux de trafic. Le système continue de faire correspondre le trafic à des règles supplémentaires pour déterminer s'il doit l'autoriser ou le refuser.
- **Règle de déchiffrement 2 : La règle Do Not Decrypt (Ne pas déchiffrer)** évalue le trafic chiffré en troisième lieu. Le trafic correspondant n'est pas déchiffré; le système inspecte ce trafic à l'aide du contrôle d'accès, mais pas de l'inspection de fichiers ou de la prévention des intrusions. Le trafic qui ne correspond pas passe à la règle suivante.

- **Règle de déchiffrement 3: La règle Block (blocage)** évalue le trafic chiffré en quatrième lieu. Le trafic correspondant est bloqué sans autre inspection. Le trafic qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 4 : Decrypt - Known Key (Déchiffrer – clé connue)** évalue le trafic chiffré en cinquième lieu. Le trafic correspondant entrant dans votre réseau est déchiffré à l'aide d'une clé privée que vous téléversez. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès gèrent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à règle de déchiffrement passe à la règle suivante.
- **Règle de déchiffrement 5 : Decrypt - Resign (Déchiffrer-Resigner)** est la règle finale. Si le trafic correspond à cette règle, le système signe de nouveau le certificat du serveur avec un certificat d'autorité de certification téléversé, puis agit comme un intermédiaire pour déchiffrer le trafic. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès traitent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à la règle SSL passe à la règle suivante.
- **Politique de déchiffrement L'action par défaut** gère tout le trafic qui ne correspond à aucun des règles de déchiffrement. L'action par défaut bloque le trafic chiffré sans autre inspection ou ne le déchiffre pas et le transmet pour l'inspection du contrôle d'accès.

Configuration de l'inspection du trafic chiffré

Vous devez créer des objets d'infrastructure à clé publique (PKI) réutilisables pour contrôler le trafic chiffré en fonction des caractéristiques de la session chiffrée et déchiffrer le trafic chiffré. Vous pouvez ajouter ces informations à la volée lors du téléversement de certificats d'autorité de certification (CA) de confiance dans u de déchiffrement puis en créant règle de déchiffrement, en créant l'objet associé pendant le processus. Cependant, la configuration de ces objets à l'avance réduit les risques de création d'objets incorrects.

Déchiffrement du trafic chiffré avec des certificats et des clés jumelées

Le système peut déchiffrer le trafic chiffré entrant si vous configurez un objet de certificat interne en téléchargeant le certificat du serveur et la clé privée utilisées pour chiffrer la session. Si vous faites référence à cet objet dans la règle u de déchiffrement avec une action **Decrypt – Known Key** (Déchiffrer - Clé connue) et que le trafic correspond à cette règle, le système utilise la clé privée téléversée pour déchiffrer la session.

Le système peut également déchiffrer le trafic sortant si vous configurez un objet d'autorité de certification interne en téléchargeant un certificat d'autorité de certification et une clé privée. Si vous faites référence à cet objet dans un règle de déchiffrement avec une action **Decrypt - Resign** (Déchiffrer - Resigner) et que le trafic correspond à cette règle, le système signe à nouveau le certificat de serveur transmis au navigateur client, puis agit comme un intermédiaire pour déchiffrer le session. Vous pouvez éventuellement remplacer uniquement la clé de certificat autosigné (et non la totalité du certificat). Dans ce cas, les utilisateurs voient un avis de clé de certificat autosigné dans le navigateur.

Contrôle du trafic en fonction des caractéristiques de session chiffrée

Le système peut contrôler le trafic chiffré en fonction de la suite de chiffrement ou du certificat de serveur utilisé pour négocier la session. Vous pouvez configurer un ou plusieurs objets réutilisables et faire référence à l'objet dans une condition règle de déchiffrement pour correspondre au trafic. Le tableau suivant décrit les différents types d'objets réutilisables que vous pouvez configurer :

Si vous configurez...	Vous pouvez contrôler le trafic chiffré selon que...
Une liste de suites de chiffrement contenant une ou plusieurs suites de chiffrement	La suite de chiffrement utilisée pour négocier la session chiffrée correspond à une suite de chiffrement dans la liste des suites de chiffrement
Un objet d'autorité de certification de confiance en chargeant un certificat d'autorité de certification de confiance de votre organisation	L'autorité de certification de confiance fait confiance au certificat du serveur utilisé pour chiffrer la session, que ce soit dans les cas suivants : • L'autorité de certification a émis le certificat directement • L'autorité de certification a délivré un certificat à une autorité de certification intermédiaire qui a émis le certificat du serveur
Un objet de certificat externe en téléchargeant un certificat de serveur	Le certificat de serveur utilisé pour chiffrer la session correspond au certificat de serveur téléchargé
Un objet de nom distinctif contenant le nom distinctif d'un sujet ou d'un émetteur de certificat	Le nom commun du sujet ou de l'émetteur, du pays, de l'organisation ou de l'unité organisationnelle sur le certificat utilisé pour chiffrer la session correspond au nom distinctif configuré.

Sujets connexes

Liste de suite de chiffrement
Nom distinctif
ICP

Évaluation de l'ordre d'une Règle de déchiffrement

Lorsque vous créez une règle de déchiffrement dans une politique de déchiffrement, vous spécifiez sa position à l'aide de la liste d'**insertion** de l'éditeur de règles. Les règles de déchiffrement dans une politique de déchiffrement sont numérotées en commençant à 1. Le système fait correspondre le trafic aux règles de déchiffrement en ordre descendant par numéro de règle croissant.

Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de déchiffrement, pour leesquelles *toutes* les conditions de la règle correspondent au trafic. Sauf dans le cas des règles Monitor (surveillance) (qui enregistrent le trafic mais n'affectent pas le flux), le système ne continue *pas* à évaluer le trafic par rapport à des règles supplémentaires de priorité inférieure une fois que le trafic correspond à une règle. Les conditions peuvent être simples ou complexes; vous pouvez contrôler le trafic par zone de sécurité, réseau ou emplacement géographique, VLAN, port, application, URL demandée, utilisateur, certificat, nom distinctif de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement.

Chaque règle possède également une *action*, qui détermine si vous surveillez, bloquez ou inspectez le trafic chiffré ou déchiffré correspondant à l'aide du contrôle d'accès. Vous observerez que le système n'inspecte *pas* davantage le trafic chiffré qu'il bloque. Il soumet le trafic chiffré et non déchiffrable au contrôle d'accès. Toutefois, les conditions des règles de contrôle d'accès exigent un trafic non chiffré, de sorte que le trafic chiffré correspond à un nombre réduit de règles.

Les règles qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées avant les règles qui utilisent des conditions *générales* (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus tardivement dans vos règles. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Astuces Un ordre adéquat de règle de déchiffrement réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles. Bien que les règles que vous créez soient uniques à chaque organisation et chaque déploiement, il existe quelques consignes générales à suivre lors de la mise en ordre des règles qui peuvent optimiser les performances tout en répondant à vos besoins.

En plus de trier les règles par numéro, vous pouvez regrouper les règles par catégories. Par défaut, le système propose trois catégories : Administrateur, Standard et Racine. Vous pouvez ajouter des catégories personnalisées, mais vous ne pouvez pas supprimer les catégories fournies par le système ni modifier leur ordre.

Sujets connexes

Options de traitement par défaut du trafic non déchiffrable
Ordre des règles SSL
Bonnes pratiques pour les règles de contrôle d'accès

Conditions de la Règle de déchiffrement

Les conditions de la règle de déchiffrement A identifient le type de trafic chiffré géré par la règle. Les conditions peuvent être simples ou complexes, et vous pouvez spécifier plusieurs types de condition par règle. Ce n'est que si le trafic répond à toutes les conditions d'une règle que la règle s'applique au trafic.

Si vous ne configurez pas de condition particulière pour une règle, le système ne correspond pas au trafic en fonction de ce critère. Par exemple, une règle avec une condition de certificat, mais aucune condition de version évalue le trafic en fonction du certificat de serveur utilisé pour négocier la session, quelle que soit la version SSL ou TLS de la session.

Chaque règle de déchiffrement est associée à une action qui détermine les éléments suivants pour la correspondance du trafic chiffré :

- Traitement : plus important encore, l'action de la règle détermine si le système surveille, fait confiance, bloque ou déchiffre le trafic chiffré qui répond aux conditions de la règle
- Journalisation : l'action de règle détermine quand et comment vous pouvez consigner les détails du trafic chiffré correspondant.

Votre configuration TLS/SSL d'inspection gère, inspecte et journalise le trafic déchiffré :

- Les actions non déchiffrables de la politique de déchiffrement gèrent le trafic que le système ne peut pas déchiffrer.
- L'action par défaut de la politique gère le trafic qui ne répond pas à une condition de règle de déchiffrement non dédiée à la surveillance.

Vous pouvez consigner un événement de connexion lorsque le système bloque ou fait confiance à une session chiffrée. Vous pouvez également forcer le système à journaliser les connexions qu'il déchiffre pour une évaluation plus approfondie par des règles de contrôle d'accès, quelle que soit la façon dont le système gère ou inspecte le trafic ultérieurement. Les journaux de connexion pour les sessions chiffrées contiennent des détails sur le chiffrement, tels que le certificat utilisé pour chiffrer cette session. Vous pouvez consigner uniquement les événements de fin de connexion, cependant :

- Pour les connexions bloquées (blocage, blocage avec réinitialisation), le système met immédiatement fin aux sessions et génère un événement

- Pour les connexions au mode Ne pas déchiffrer, le système génère un événement à la fin de la session

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). u de déchiffrement) redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Notez qu'une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Sujets connexes

Conditions des règles de zone de sécurité
Conditions des règles de réseau
Conditions de règle des balises VLAN
Conditions des règles d'utilisateur
Conditions des règles d'application
Conditions de règle de port
Conditions de règle de catégorie, à la page 19
Conditions basées sur le certificat de serveur de Règle de déchiffrement, à la page 20

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions des règles d'utilisateur

Les conditions des règles d'utilisateur correspondent au trafic en fonction de l'utilisateur qui initie la connexion ou du groupe auquel l'utilisateur appartient. Par exemple, vous pouvez configurer une règle de blocage pour interdire à tout membre du groupe des finances d'accéder à une ressource réseau.

Pour les règles de contrôle d'accès uniquement, vous devez d'abord associer une politique d'identité à la politique de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès.

En plus de configurer les utilisateurs et les groupes pour les domaines configurés, vous pouvez définir des politiques pour les utilisateurs d'identités spéciales suivants :

- Échec de l'authentification : utilisateur qui a échoué à l'authentification avec le portail captif.
- Invité : utilisateurs configurés comme utilisateurs invités dans le portail captif.
- Aucune authentification requise : utilisateurs qui correspondent à une action de règle **Aucune authentification requise n'est requise**.
- Inconnu : utilisateurs qui ne peuvent pas être identifiés; par exemple, les utilisateurs qui ne sont pas téléchargés par un domaine configuré.

Conditions des règles d'application

Lorsque le système analyse le trafic IP, il peut identifier et classer les applications couramment utilisées sur votre réseau. Cette *connaissance des applications* basée sur la découverte constitue la base du *contrôle des applications*, c'est-à-dire la capacité de contrôler le trafic des applications.

Les *filtres d'applications* fournis par le système vous aident à effectuer le contrôle des applications en organisant les applications en fonction de caractéristiques de base: type, risque, pertinence commerciale, catégorie et

balises. Vous pouvez créer des filtres définis par l'utilisateur réutilisables en fonction de combinaisons de filtres fournis par le système ou de combinaisons personnalisées d'applications.

Au moins un détecteur doit être activé pour chaque condition de règle d'application dans la politique. Si aucun détecteur n'est activé pour une application, le système active automatiquement tous les détecteurs fournis par le système pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application. Pour en savoir plus sur les détecteurs d'application, consultez Principes fondamentaux des détecteurs d'applications.

Vous pouvez utiliser à la fois des filtres d'application et des applications spécifiées individuellement pour assurer une couverture complète. Cependant, lisez la note suivante avant de commander vos règles de contrôle d'accès.

Avantages des filtres d'application

Les filtres d'applications vous aident à configurer rapidement le contrôle des applications. Par exemple, vous pouvez facilement utiliser les filtres fournis par le système pour créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible intérêt pour l'entreprise. Si un utilisateur tente d'utiliser l'une de ces applications, le système bloque la session.

L'utilisation de filtres d'application simplifie la création et l'administration des politiques. Cela vous garantit que le système contrôle le trafic des applications comme prévu. Étant donné que Cisco met fréquemment à jour et ajoute des détecteurs d'applications par l'intermédiaire des mises à jour du système et de la base de données de vulnérabilités (VDB), vous pouvez vous assurer que le système utilise des détecteurs à jour pour surveiller le trafic des applications. Vous pouvez également créer vos propres détecteurs et attribuer des caractéristiques aux applications qu'ils détectent, en les ajoutant automatiquement aux filtres existants.

Caractéristiques des applications

Le système caractérise chaque application qu'il détecte à l'aide des critères décrits dans le tableau suivant. Utilisez ces caractéristiques comme filtres d'application.

Tableau 1 : Caractéristiques des applications

Caractéristiques	Description	Exemple
Type	Les protocoles d'application représentent les communications entre les hôtes. Les clients représentent des logiciels exécutés sur un hôte. Les applications Web représentent le contenu ou l'URL demandée pour le trafic HTTP.	HTTP et SSH sont des protocoles d'application. Les navigateurs Web et les clients de courriel sont des clients. MPEG video et Facebook sont des applications Web.
Risque	La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation.	Les applications homologue à homologue ont tendance à présenter un risque très élevé.
Pertinence commerciale	La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation, plutôt qu'à des fins récréatives.	Les applications de jeu ont généralement une très faible pertinence commerciale.

Caractéristiques	Description	Exemple
Type	Une classification générale de l'application qui décrit sa fonction la plus essentielle. Chaque application appartient à au moins une catégorie.	Facebook fait partie de la catégorie des réseaux sociaux.
Balise	Des informations supplémentaires sur l'application. Les applications peuvent avoir un nombre illimité de balises, y compris aucune.	Les applications Web de vidéo en flux continu sont souvent marquées pour `une bande passante élevée` et `affichent des publicités`.

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications

Conditions de règle de port

Les conditions de port vous permettent de contrôler le trafic en fonction de ses ports source et de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic.

Le filtrage des applications est également recommandé pour les applications, comme FTD, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port source dans une seule règle de contrôle d'accès.

Conditions de règle de catégorie

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations

d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise.

Pour en savoir plus, consultez Présentation du filtrage d'URL.

Si vous utilisez des conditions de règle de catégorie dans Politiques de déchiffrement dans une règle avec l'action de règle **Ne pas déchiffrer**, consultez Action Ne pas déchiffrer de la Règle de déchiffrement, à la page 34.

Conditions basées sur le certificat de serveur de Règle de déchiffrement

Les règles de déchiffrement peuvent gérer et déchiffrer le trafic chiffré en fonction des caractéristiques du certificat de serveur. Vous pouvez configurer les règles de déchiffrement en fonction des attributs de certificat de serveur suivants :

- Les conditions de nom distinctif vous permettent de gérer et d'inspecter le trafic chiffré en fonction de l'autorité de certification qui a émis un certificat de serveur, ou le détenteur du certificat. En fonction du nom distinctif de l'émetteur, vous pouvez gérer le trafic en fonction de l'autorité de certification qui a émis le certificat de serveur de site.
- Les conditions de certificat de règles de déchiffrement vous permettent de gérer et d'inspecter le trafic chiffré en fonction du certificat de serveur utilisé pour chiffrer ce trafic. Vous pouvez configurer une condition avec un ou plusieurs certificats; correspond à la règle si le certificat correspond à l'un des certificats de la condition.
- Les conditions d'état de certificat dans règles de déchiffrement vous permettent de gérer et d'inspecter le trafic chiffré en fonction de l'état du certificat de serveur utilisé pour chiffrer le trafic, notamment si un certificat est valide, révoqué, expiré, non encore valide, autosigné, signé par un autorité de certification de confiance, si la liste de révocation de certificats (CRL) est valide; si l'indication du nom du serveur (SNI) dans le certificat correspond au serveur de la demande.
- Les conditions de suite de chiffrement dans règles de déchiffrement vous permettent de gérer et d'inspecter le trafic chiffré en fonction de la suite de chiffrement utilisée pour négocier la session chiffrée.
- Les conditions de session dans règles de déchiffrement vous permettent d'inspecter le trafic chiffré en fonction de la version SSL ou TLS utilisée pour chiffrer le trafic.

Pour détecter plusieurs suites de chiffrement dans une règle, l'émetteur du certificat ou le détenteur du certificat, vous pouvez créer des objets réutilisables de listes de suite de chiffrement et de nom unique, et les ajouter à votre règle. Pour détecter le certificat de serveur et certains états de certificat, vous devez créer des objets certificat externe et autorité de certification externe pour la règle.

Sujets connexes

Conditions de Règle de déchiffrement du certificat, à la page 21
Conditions de Règle de déchiffrement d'état du certificat, à la page 27
Confiance accordée aux autorités de certification externes, à la page 26
Trafic correspondant à l'état du certificat
Conditions de la suite de chiffrement de Règle de déchiffrement, à la page 30
Conditions de la version du protocole de chiffrement de Règle de déchiffrement, à la page 33

Conditions de Règle de déchiffrement du certificat

Lorsque vous générez une condition de règle de déchiffrement basée sur un certificat, vous pouvez télécharger un certificat de serveur. Vous enregistrez le certificat en tant *qu'objet* de certificat externe, qui est réutilisable et associe un nom à un certificat de serveur. Par ailleurs, vous pouvez configurer des conditions de certificat avec des objets de certificat externes et des groupes d'objets existants.

Vous pouvez rechercher le champ **Certificats disponibles** dans la règle de condition basée sur les objets de certificat externes et les groupes d'objets en fonction des caractéristiques de nom distinctif de certificat suivantes :

- Nom commun (CN) du sujet ou de l'émetteur, ou si l'URL est contenue dans l'autre nom du sujet (SAN)du certificat

  L'URL que l'utilisateur saisit dans le navigateur correspond au nom commun (CN)

- Organisation du sujet ou de l'émetteur (O)
- Unité organisationnelle (UO) du sujet ou de l'émetteur

Vous pouvez choisir d'effectuer la mise en correspondance avec plusieurs certificats dans une seule condition de règle de certificat; si le certificat utilisé pour chiffrer le trafic correspond à l'un des certificats téléchargés, le trafic chiffré correspond à la règle.

Vous pouvez ajouter un maximum de 50 objets de certificat externes et groupes d'objets de certificat externes aux certificats **sélectionnés** dans une seule condition de certificat.

Tenez compte des points suivants :

- Vous ne pouvez pas configurer de condition de certificat si vous sélectionnez également l'action **Déchiffrer - Clé connue**. Étant donné que cette action vous oblige à sélectionner un certificat de serveur pour déchiffrer le trafic, cela signifie que le certificat correspond déjà au trafic.
- Si vous configurez une condition de certificat avec un objet de certificat externe, toute suite de chiffrement que vous ajoutez à une condition de suite de chiffrement, ou tout objet d'autorité de certification interne que vous associez à l'action **Déchiffrer – Resigner**, doit correspondre au type d'algorithme de signature du certificat externe. Par exemple, si la condition de certificat de votre règle fait référence à un certificat de serveur basé sur EC, toutes les suites de chiffrement que vous ajoutez, ou les certificats d'autorité de certification que vous associez à l'action **Déchiffrer – Resigner**, doivent également être basés sur EC. Si vos types d'algorithmes de signature ne correspondent pas dans ce cas, l'éditeur de politiques affiche un avertissement à côté de la règle.
- La première fois que le système détecte une session chiffrée sur un nouveau serveur, les données de certificat ne sont pas disponibles pour le traitement de ClientHello, ce qui peut faire en sorte que la première session soit déchiffrée. Après la session initiale, le périphérique géré met en cache les données du message de certificat du serveur. Pour les connexions ultérieures à partir du même client, le système peut faire correspondre le message ClientHello de manière concluante aux règles avec conditions de certificat et traiter le message pour maximiser le potentiel de déchiffrement.

Conditions de règles de noms distinctifs (DN)

Cette rubrique explique comment utiliser les conditions de nom distinctif dans une règle de déchiffrement. Si vous n'êtes pas sûr, vous pouvez trouver le nom de sujet (SAN) et le nom commun d'un certificat à l'aide d'un navigateur Web, puis vous pouvez ajouter ces valeurs à un règle de déchiffrement en tant que conditions de nom distinctif.

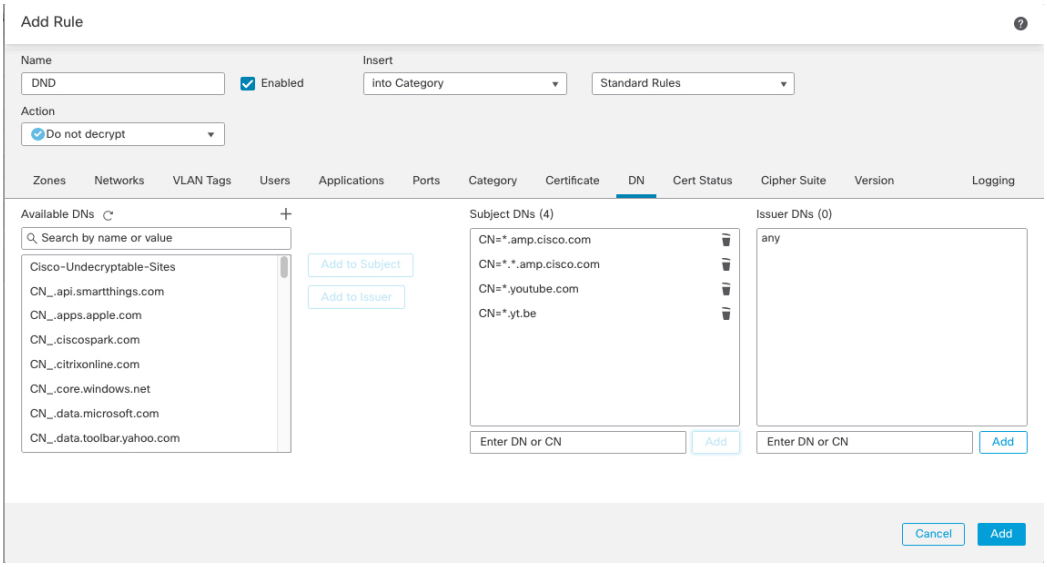
Pour en savoir plus sur les SAN, consultez RFC 528, section 4.2.1.6.

Les sections suivantes traitent :

- Exemple de correspondance de règle de nom distinctif
- Comment le système utilise le SNI et le SAN
- Comment trouver le nom commun d'un certificat et les autres noms de son sujet
- Comment ajouter une condition de règle de nom distinctif

Exemple de correspondance de règle de nom distinctif

Voici un exemple des conditions de règle de nom distinctif dans une règle Ne pas déchiffrer. Supposons que vous souhaitez vous assurer de *ne pas* déchiffrer le trafic vers `amp.cisco.com` ou YouTube. Vous pouvez configurer vos conditions de nom distinctif comme suit :



Les conditions de règle de DN précédentes correspondraient aux URL suivantes et, par conséquent, le trafic serait déchiffré, une règle antérieure l'a empêché :

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

Les conditions de règle de nom distinctif précédentes *ne* correspondraient à aucune des URL suivantes et, par conséquent, le trafic ne correspondrait pas à la règle Ne pas déchiffrer, mais pourrait correspondre à tout autre règles de déchiffrement dans le même politique de déchiffrement.

- amp.cisco.com

- youtube.com
- yt.be

Pour mettre en correspondance l'un des noms d'hôte précédents, ajoutez d'autres nœuds de commande à la règle (par exemple, l'ajout de `CN=yt.be` correspondrait à cette URL.)

Comment le système utilise le SNI et le SAN

La partie nom d'hôte de l'URL dans la demande du client constitue l'indication SNI (Server Name Indication). Le client spécifie le nom d'hôte auquel il souhaite se connecter (par exemple, `auth.amp.cisco.com`) en utilisant l'extension SNI dans l'établissement de liaison TLS. Le serveur sélectionne ensuite la clé privée et la chaîne de certificats correspondantes, qui sont nécessaires pour établir la connexion tout en hébergeant tous les certificats sur une seule adresse IP.

S'il y a une correspondance entre le SNI et le nom de domaine ou un réseau SAN dans le certificat, nous utilisons le SNI pour la comparaison avec les noms de domaine répertoriés dans la règle. S'il n'y a pas de SNI ou s'il ne correspond pas au certificat, nous utilisons le nom distinctif du certificat pour la comparaison avec les noms distinctifs répertoriés dans la règle.

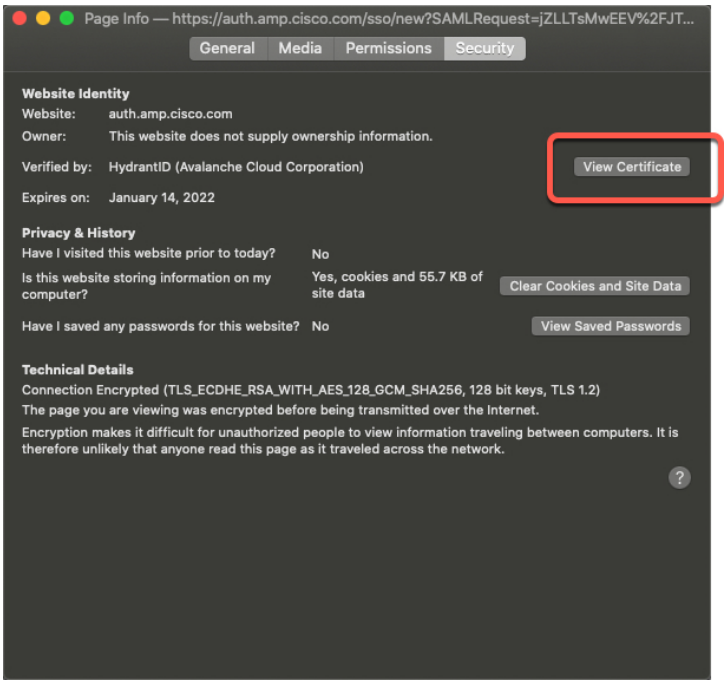
Comment trouver le nom commun d'un certificat et les autres noms de son sujet

Pour trouver le nom commun d'un certificat, procédez comme suit. Vous pouvez même utiliser ces étapes pour trouver le nom commun et les SAN d'un certificat autosigné.

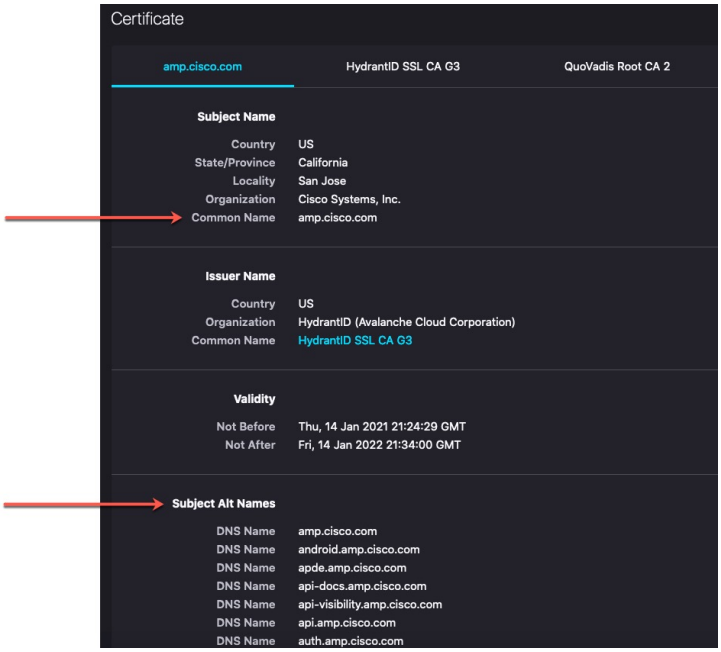
Ces étapes s'appliquent à Firefox, mais celles des autres navigateurs sont similaires. La procédure suivante utilise `amp.cisco.com` comme exemple.

1. Accédez à `amp.cisco.com` dans Firefox.
2. Dans la barre d'emplacement du navigateur, à gauche de l'URL, cliquez sur  .
3. Cliquez sur **Connexion sécurisée** > **Plus d'informations**.

   (Pour un certificat non sécurisé ou autosigné, cliquez sur **Connexion non sécurisée** > **Plus d'informations**.)
4. Dans la boîte de dialogue Informations sur la page , cliquez sur **Afficher le certificat**.



5. La page suivante affiche les détails du certificat.



Tenez compte des points suivants :

- `CN=auth.amp.cisco.com`, s'il est utilisé comme condition de règle de DN, ne correspondrait *qu'à* ce nom d'hôte (c'est-à-dire SNI). Le SNI `amp.cisco.com` ne correspondrait *pas*.
- Pour correspondre à autant de champs de nom de domaine que possible, utilisez des caractères génériques.

Par exemple, pour trouver une correspondance à `auth.amp.cisco.com`, utilisez `CN=*.amp.cisco.com`. Pour mettre en correspondance `auth.us.amp.cisco.com`, utilisez `CN=*.*.amp.cisco.com`.

Un DN comme `CN=*.example.com` correspond à `www.example.com` mais *pas* à `example.com`. Pour faire correspondre les deux SNI, utilisez deux DN dans la condition de règle.

- Cependant, n'exagérez pas l'usage des caractères génériques. Par exemple, un objet DN comme `CN=*.google.com` correspond à un très grand nombre de SAN. Au lieu de `CN=*.google.com`, utilisez un objet DN comme `CN=*.youtube.com` comme objet DN afin qu'il corresponde à des noms comme `www.youtube.com`.

  Vous pouvez également utiliser des variantes du SNI qui correspondent aux SAN, comme `CN=*.youtube.com`, `CN=youtu.be`, `CN=*.yt.be`,etc.

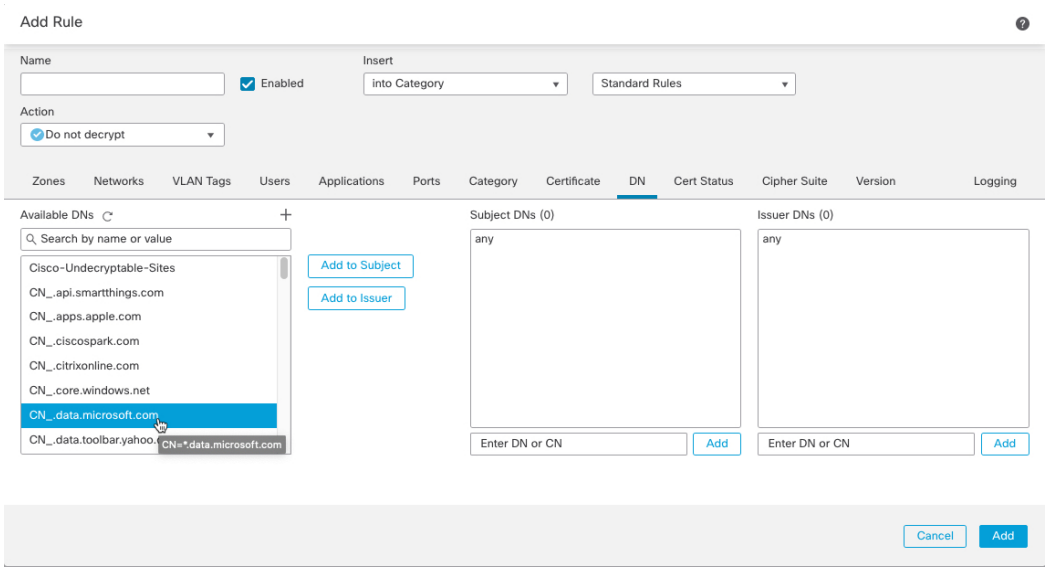
- Un certificat autosigné devrait fonctionner de la même manière. Vous pouvez confirmer qu'il s'agit d'un certificat autosigné par le fait que le DN de l'émetteur est le même que le DN du sujet.

Comment ajouter une condition de règle de nom distinctif

Une fois que vous connaissez le numéro de référence que vous souhaitez mettre en correspondance, modifiez le règle de déchiffrement de l'une des manières suivantes :

- Utilisez un nom distinctif existant.

  Cliquez sur le nom d'un DN, puis sur **Add to Subject** ou **Add to Issuer** (Ajouter à l'objet ou Ajouter à l'émetteur). (**Ajouter à l'objet** est beaucoup plus courant.) Pour afficher la valeur d'un objet DN, passez le pointeur de la souris dessus.)

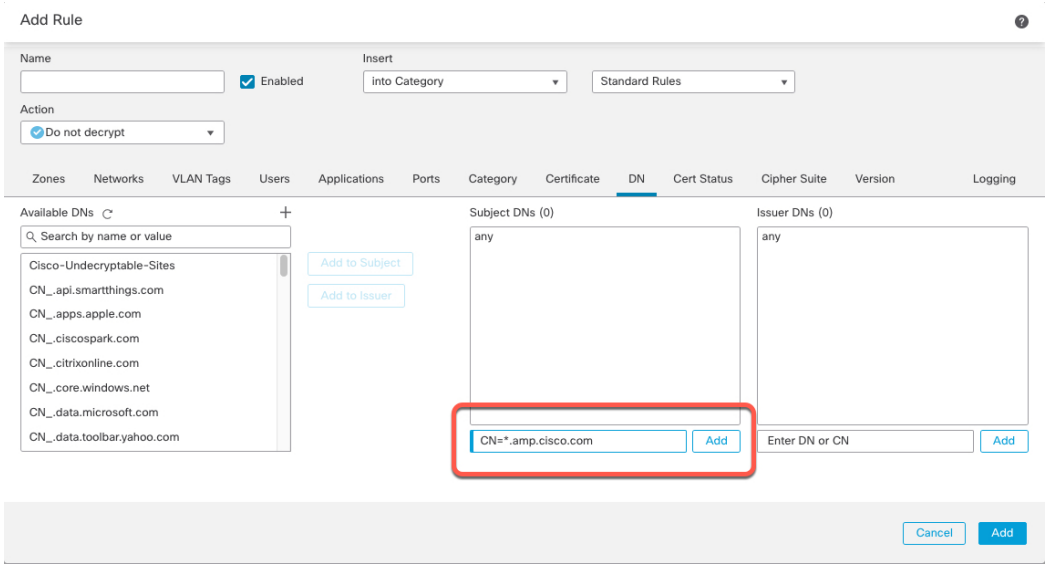


- Créez un nouvel objet DN.

  Cliquez sur **Ajouter** (+) à droite de l'option Noms distinctifs disponibles. L'objet DN doit comprendre un nom et une valeur.

- Ajoutez directement le DN.

Saisissez le nom distinctif dans la partie inférieure du champ **Subject DNs** ou **Issuer DNs** (DN de l'objet ou de l'émetteur). (**Les DN de l'objet** sont plus courants.) Après avoir saisi le DN, cliquez sur **Add** (Ajouter).



Sujets connexes

Nom distinctif

Confiance accordée aux autorités de certification externes

Vous pouvez faire confiance aux autorités de certification en ajoutant des certificats d'autorité de certification racine et intermédiaire à votre politique de déchiffrement, puis utiliser ces autorités de certification de confiance pour vérifier les certificats de serveur utilisés pour chiffrer le trafic.

Si un certificat d'autorité de certification de confiance contient une liste de révocation de certificats (CRL) téléchargée, vous pouvez également vérifier si une autorité de certification de confiance a révoqué le certificat de chiffrement.

Astuces Chargez tous les certificats de la chaîne de confiance d'une autorité de certification racine dans la liste des certificats d'autorités de certification de confiance, y compris le certificat de l'autorité de certification racine et tous les certificats d'autorités de certification intermédiaires. Sinon, il est plus difficile de détecter les certificats de confiance émis par des autorités de certification intermédiaires. En outre, si vous configurez des conditions d'état de certificat pour faire confiance au trafic en fonction de l'autorité de certification émettrice racine, tout le trafic au sein de la chaîne de confiance d'une autorité de certification de confiance peut être autorisé sans déchiffrement, plutôt que de le déchiffrer inutilement.

Pour en savoir plus, consultez Objet autorité de certification de confiance.

Remarque Lorsque vous créez u de déchiffrement, plusieurs **certificats d'autorité de certification de confiance** de la politique sont remplis avec plusieurs certificats d'autorité de certification de confiance, y compris le groupe **Cisco-Trusted-Authorities**, qui est ajouté à la liste **Select Trusted CAs** (Sélectionner des AC de confiance).

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **Edit** (✎) à côté de politique de déchiffrement pour modifier.

Étape 3 Cliquez sur **Ajouter une règle** pour ajouter une nouvelle règle de déchiffrement ou cliquez sur **Edit** (✎) pour modifier une règle existante.

Étape 4 Cliquez sur l'onglet **Certificats**.

Étape 5 Recherchez les autorités de certification de confiance que vous souhaitez ajouter à partir des **certificats disponibles**, comme suit :

- Pour ajouter un objet autorité de certification de confiance à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la liste des **certificats disponibles** .
- Pour rechercher des objets et des groupes d'autorités de certification de confiance à ajouter, cliquez sur l'invite **de recherche par nom ou par valeur** au-dessus de la liste des **certificats disponibles** , puis saisissez le nom de l'objet ou une valeur de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.

Étape 6 Pour sélectionner un objet, cliquez dessus. Pour sélectionner tous les objets, cliquez avec le bouton droit, puis **sélectionnez tout**.

Étape 7 Cliquez sur **Add Rule** (ajouter une règle).

Astuces Vous pouvez également faire glisser et déposer les objets sélectionnés.

Étape 8 Ajoutez la règle ou continuez à la modifier.

Prochaine étape

- Ajoutez une condition d'état de certificat règle de déchiffrement à votre règle SSL. Consultez la Trafic correspondant à l'état du certificat pour de plus amples renseignements.
- Déployer les changements de configuration.

Conditions de Règle de déchiffrement d'état du certificat

Pour chaque état de certificat de règle de déchiffrement que vous configurez, vous pouvez comparer le trafic à la présence ou à l'absence d'un état donné. Vous pouvez sélectionner plusieurs statuts dans une condition de règle; si le certificat correspond à l'un des états sélectionnés, la règle correspond au trafic.

Vous pouvez choisir d'établir une correspondance avec la présence ou l'absence de plusieurs états de certificat dans une seule condition de règle d'état de certificat; le certificat doit correspondre à un seul des critères pour correspondre à la règle.

Vous devez déterminer, lors de la définition de ce paramètre, si vous configurez une règle de déchiffrement ou de blocage. En règle générale, vous devez cliquer sur **Yes** (oui) pour une règle de blocage et sur **No** pour une règle de déchiffrement. Exemples :

- Si vous configurez une règle **Decrypt – Resign**, le comportement par défaut est de déchiffrer le trafic avec un certificat expiré. Pour modifier ce comportement, cliquez sur **Non** pour **Expiré**) pour que le trafic avec un certificat expiré ne soit pas déchiffré et signé.
- Si vous configurez une règle de **Déchiffre - Resigner**, le comportement par défaut est d'autoriser le trafic avec un certificat expiré. Pour modifier ce comportement, cliquez sur **Yes** (oui) pour **Expiré** afin que le trafic avec un certificat expiré soit bloqué.

Le tableau suivant décrit comment le système évalue le trafic chiffré en fonction de l'état du certificat du serveur de chiffrement.

Tableau 2 : Critères de condition de la règle d'état du certificat

Vérification de l'état	État défini sur Yes (oui)	État défini sur No (non)
Retiré	La politique fait confiance à l'autorité de certification qui a émis le certificat de serveur, et le certificat d'autorité de certification téléchargé dans la politique contient une liste de révocation de certificats de serveur.	La politique fait confiance à l'autorité de ce qui a émis le certificat de serveur, et le cert d'autorité de certification téléchargé dans la ne contient pas de liste de révocation de ce
Autosigné	Le certificat de serveur détecté contient le même nom distinctif d'émetteur et de sujet.	Le certificat de serveur détecté contient dif noms distinctifs d'émetteur et de sujet.
Valide	Toutes les conditions suivantes sont vraies : • La politique fait confiance à l'autorité de certification qui a émis le certificat. • La signature est valide. • L'émetteur est valide. • Aucune des autorités de certification de confiance de la politique n'a révoqué le certificat. • La date actuelle est comprise entre la date de début de validité du certificat et la date de fin de validité du certificat.	Au moins une des conditions suivantes est • La politique ne fait pas confiance à l'a certification qui a émis le certificat. • La signature est non valide. • L'émetteur n'est pas valide. • Une autorité de certification de confia la politique a révoqué le certificat. • La date actuelle est antérieure à la date du certificat. • La date actuelle est postérieure à la da validité du certificat.
Signature non valide	La signature du certificat ne peut pas être correctement validée par rapport au contenu du certificat.	La signature du certificat est correctement v rapport au contenu du certificat.
Émetteur non valide	Le certificat de l'autorité de certification émettrice n'est pas stocké dans la liste des certificats d'autorités de certification de confiance de la politique.	Le certificat de l'autorité de certification ém stocké dans la liste des certificats d'autorit certification de confiance de la politique.
Expiré	La date actuelle est postérieure à la date de validité du certificat.	La date actuelle est antérieure à la date de v certificat ou est la date de validité du certif
Non encore valide	La date actuelle est antérieure à la date de validité du certificat.	La date actuelle est postérieure ou égale à validité du certificat.

Vérification de l'état	État défini sur Yes (oui)	État défini sur No (non)
Certificat non valide	Le certificat est non valide. Au moins une des conditions suivantes est vraie : • Extension de certificat non valide ou incohérente; c'est-à-dire qu'une extension de certificat avait une valeur non valide (par exemple, un encodage incorrect) ou une valeur incohérente avec d'autres extensions. • Le certificat ne peut pas être utilisé pour l'objectif spécifié. • Le paramètre de longueur du chemin de contraintes de base a été dépassé. Pour en apprendre davantage à ce sujet, consultez RFC 5280, section 4.2.1,9. • La valeur du certificat Pas avant ou Pas après n'est pas valide. Ces dates peuvent être codées au format UTCTime ou GeneralizedTime Pour en savoir plus, consultez la RFC 5280, section 4.1.2.5. • Le format de la contrainte de nom n'est pas reconnu; par exemple, un format d'adresse de courriel d'une forme non mentionnée dans la section 4.2.1.10 de la RFC 5280. Cela peut être dû à une extension inappropriée ou à une nouvelle fonctionnalité non prise en charge actuellement. Un type de contraintes de nom non pris en charge a été rencontré. OpenSSL prend actuellement en charge uniquement les types de nom de répertoire, de nom DNS, de courriel et d'URI. • L'autorité de certification racine n'est pas approuvée pour l'objectif précisé. • L'autorité de certification racine rejette l'objectif spécifié.	Le certificat est valide. Toutes les condit sont vraies : • Extension de certificat valide • Le certificat peut être utilisé aux fi • Longueur du chemin de contrainte valide • Valeurs valides pour Pas avant et • Contrainte de nom valide • Le certificat racine est sécurisé po spécifié. • Le certificat racine accepte l'objec

Vérification de l'état	État défini sur Yes (oui)	État défini sur No (non)
CRL non valide	La signature numérique de la liste de révocation de certificats (CRL) n'est pas valide. Au moins une des conditions suivantes est vraie : • La valeur du champ Prochaine mise à jour ou Dernière mise à jour de la liste de révocation de certificats n'est pas valide. • La liste de révocation de certificats n'est pas encore valide. • La liste de révocation de certificats a expiré. • Une erreur est survenue lors de la tentative de vérification du chemin de la liste de révocation de certificats. Cette erreur se produit uniquement si la vérification étendue des CRL est activée. • La liste de révocation de certificats est introuvable. • Les seules listes de révocation de certificats qui ont pu être trouvées ne correspondaient pas à la portée du certificat.	La liste de révocation de certificats est vali les conditions suivantes sont vraies : • Les champs Prochaine mise à jour et mise à jour sont valides. • La date de la liste de révocation de cer valide. • Le chemin d'accès est valide. • La liste de révocation de certificats a é • La liste de révocation de certificats co à la portée du certificat.
Non-concordance du serveur	Le nom du serveur ne correspond pas au nom SNI (Server Name Indication ou SNI) du serveur, ce qui pourrait indiquer une tentative d'usurpation du nom du serveur.	Le nom du serveur correspond au nom SNI auquel le client demande l'accès.

Notez que même si un certificat correspond à plus d'un état, la règle fait qu'une action n'est entreprise sur le trafic qu'une seule fois.

Pour vérifier si une autorité de certification a émis ou révoqué un certificat, il faut téléverser les certificats d'autorité de certification racine et intermédiaire et les CRL associées en tant qu'objets. Vous ajoutez ensuite ces objets d'autorité de certification de confiance à la liste de certificats d'autorité de certification de confiance de politique de déchiffrement.

Conditions de la suite de chiffrement de Règle de déchiffrement

Le système fournit des suites de chiffrement prédéfinies que vous pouvez ajouter à une condition de règle de suite de chiffrement. Vous pouvez également ajouter des objets de liste de suite de chiffrement contenant plusieurs suites de chiffrement.

Remarque Vous ne pouvez pas ajouter de nouvelles suites de chiffrement. Vous ne pouvez ni modifier ni supprimer les suites de chiffrement prédéfinies.

Vous pouvez ajouter un maximum de 50 suites et listes de suites de chiffrement aux suites de chiffrement **sélectionnées** dans une condition de suite de chiffrement unique. Le système prend en charge l'ajout des suites de chiffrement suivantes à une condition de suite de chiffrement :

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

Tenez compte des points suivants :

- Si vous ajoutez des suites de chiffrement non prises en charge à votre déploiement, vous ne pouvez pas déployer votre configuration. Par exemple, les déploiements passifs ne prennent pas en charge le déchiffrement du trafic à l'aide des suites de chiffrement Diffie-Hellman éphémères (DHE) ou ECDHE (éphémères elliptiques à courbe Diffie-Hellman). La création d'une règle avec ces suites de chiffrement vous empêche de déployer votre politique de contrôle d'accès.
- Si vous configurez une condition de suite de chiffrement avec une suite de chiffrement, tous les objets de certificat externe que vous ajoutez à une condition de certificat, ou tout objet d'autorité de certification interne que vous associez à l'action **Déchiffrer – Resigner**, doivent correspondre au type d'algorithme de signature de la suite de chiffrement. Par exemple, si la condition de suite de chiffrement de votre règle fait référence à une suite de chiffrement basée sur EC, tous les certificats de serveur que vous ajoutez ou les certificats d'autorité de certification que vous associez à l'action **Déchiffrer - Resigner** doivent également être basés sur EC. Si vous ne correspondez pas aux types d'algorithmes de signature dans ce cas, l'éditeur de politiques affiche une icône d'avertissement à côté de la règle.

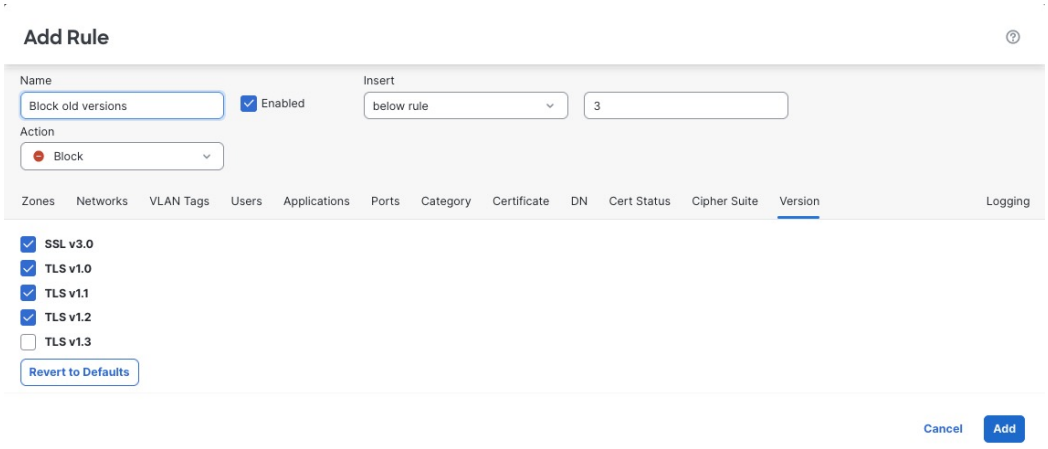
- Vous pouvez ajouter une suite de chiffrement anonyme à la condition **Cipher Suite** dans une règle SSL, mais gardez à l'esprit :
  - Le système supprime automatiquement les suites de chiffrement anonymes pendant le traitement de ClientHello. Pour que le système utilise la règle, vous devez également configurer vos dans un ordre qui empêche le traitement de ClientHello. Pour en savoir plus, consultez Ordre des règles SSL.
  - Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car le système ne peut pas déchiffrer le trafic chiffré à l'aide d'une suite de chiffrement anonyme.
- Lorsque vous définissez une suite de chiffrement comme condition de règle, il faut tenir compte du fait que la règle correspond à la suite de chiffrement négociée dans le message ServerHello, plutôt qu'à la liste complète des suites de chiffrement spécifiées dans le message ClientHello. Pendant le traitement de ClientHello, le périphérique géré élimine les suites de chiffrement non prises en charge du message ClientHello. Toutefois, si toutes les suites de chiffrement spécifiées sont supprimées, le système conserve la liste d'origine. Si le système conserve des suites de chiffrement non prises en charge, l'évaluation ultérieure donne lieu à une session non déchiffrée.

Conditions de la version du protocole de chiffrement de Règle de déchiffrement

Vous pouvez choisir d'effectuer la mise en correspondance avec le trafic chiffré à l'aide de SSL version 3.0 ou TLS version 1.0, 1.1 ou 1.2. Par défaut, toutes les versions de protocole sont sélectionnées lorsque vous créez une règle; si vous sélectionnez plusieurs versions, le trafic chiffré qui correspond à l'une des versions sélectionnées correspond à la règle. Vous devez sélectionner au moins une version de protocole lors de l'enregistrement de la condition de règle.

Vous ne pouvez pas sélectionner SSL v2.0 dans une condition de règle de version; le système ne prend pas en charge le déchiffrement du trafic chiffré avec SSL version 2.0. Vous pouvez configurer une action non déchiffrable pour autoriser ou bloquer ce trafic sans autre inspection.

Par exemple, pour bloquer tout le trafic SSL v1.0, TLS v1.0 et TLS v1.1, définissez les options comme suit :



Actions de Règle de déchiffrement

Les sections suivantes traitent des actions disponibles avec les Règles de déchiffrement.

Action Monitor (Surveiller) de Règle de déchiffrement

L'action **Monitor** (Surveiller) n'est pas conçue pour autoriser ou refuser le trafic. Son objectif principal est plutôt de forcer la journalisation de la connexion, quelle que soit la façon dont le trafic correspondant est finalement géré. Le message ClientHello n'est pas modifié si le trafic correspond à une condition de règle **Monitor**.

Le trafic est ensuite comparé à des règles supplémentaires, le cas échéant, pour déterminer s'il faut le faire confiance, le bloquer ou le déchiffrer. La première règle non relative à Monitor mise en correspondance détermine le flux de trafic et toute inspection ultérieure. En l'absence de règles de correspondance supplémentaires, le système utilise l'action par défaut.

Comme le but principal des règles Monitor est de suivre le trafic réseau, le système consigne automatiquement les événements de fin de connexion pour le trafic surveillé dans la base de données Cisco Secure Firewall Management Center, quelle que soit la configuration de journalisation de la règle ou de l'action par défaut qui gère ultérieurement la connexion.

Action Ne pas déchiffrer de la Règle de déchiffrement

L'action **Ne pas déchiffrer** transmet le trafic chiffré à l'évaluation par les règles de la politique de contrôle d'accès et l'action par défaut. Étant donné que certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, ce trafic peut correspondre à moins de règles. Le système ne peut pas effectuer d'inspection approfondie sur le trafic chiffré, comme une inspection de prévention des intrusions ou de fichier.

Les raisons typiques d'une action de règle **Ne pas déchiffrer** comprennent :

- Lorsque le déchiffrement, du trafic TLS/SSL est interdit par la loi.
- Des sites en lesquels vous pouvez avoir confiance.
- Sites que vous pouvez perturber en inspectant le trafic (comme Windows Update).
- Pour afficher les valeurs des champs TLS/SSL à l'aide des événements de connexion. (Vous n'avez pas besoin de déchiffrer le trafic pour afficher les champs d'événement de connexion.) .

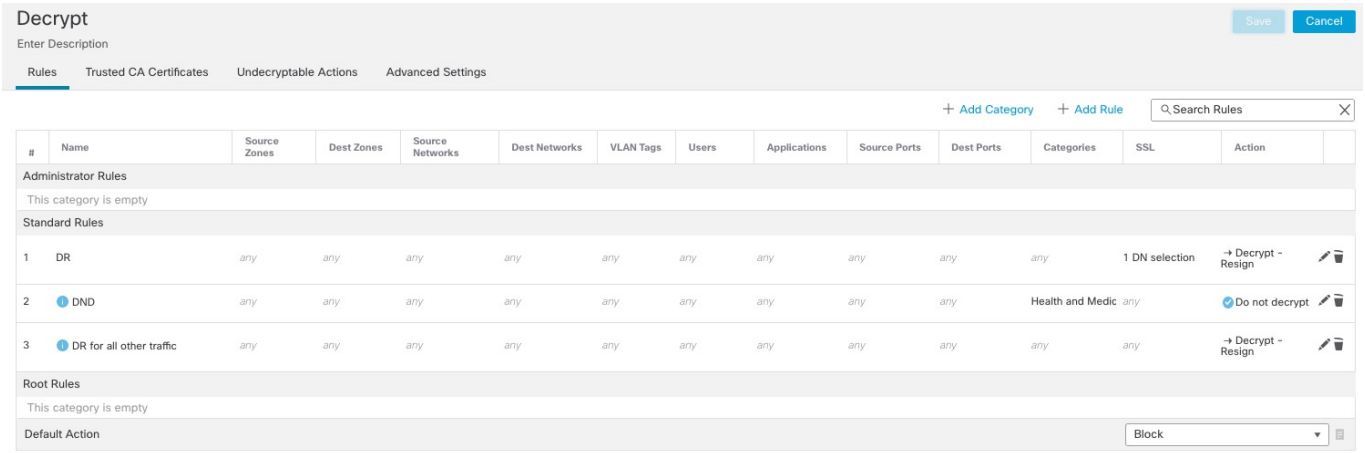
Pour en savoir plus, consultez Options de traitement par défaut du trafic non déchiffrable

Limites des catégories dans les règles Ne pas déchiffrer

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise. Bien que nous nous efforcions de mettre à jour et d'améliorer continuellement les catégories de filtrage d'URL, ce n'est pas une science exacte. Certains sites Web ne sont pas du tout classés et il est possible que certains sites Web soient mal classés.

éviter d'utiliser trop de catégories dans les règles « ne pas déchiffrer » pour éviter le déchiffrement du trafic sans raison; Par exemple, la catégorie Santé et Médecine comprend le site Web WebMD, qui ne menace pas la vie privée des patientes.

Vous trouverez ci-dessous un exemple de politique de déchiffrement qui peut empêcher le déchiffrement des sites Web de la catégorie Santé et Médecine, mais autoriser le déchiffrement pour WebMD et tout le reste. Vous trouverez des renseignements généraux sur les règles de déchiffrement dans Directives pour l'utilisation du déchiffrement TLS/SSL, à la page 2.



Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications.

Actions de blocage de Règle de déchiffrement

Le système effectue les actions règle de déchiffrement suivantes pour le trafic que vous ne souhaitez pas faire passer par le système :

- **Bloquer** pour mettre fin à la connexion, ce qui entraîne une erreur dans le navigateur client.

  Le message d'erreur n'indique pas que le site a été bloqué en raison de la politique. Au lieu de cela, des erreurs peuvent indiquer qu'il n'y a pas d'algorithmes de chiffrement communs. Il n'est pas évident dans ce message que vous ayez délibérément bloqué la connexion.

- **Bloquez avec réinitialisation** pour mettre fin à la connexion et la réinitialiser, ce qui entraîne une erreur dans le navigateur client.

  L'erreur indique que la connexion a été réinitialisée, mais n'indique pas pourquoi.

Astuces Vous ne pouvez pas utiliser l'action **Block** (bloquer) ou **Block with reset** (bloquer avec réinitialisation) dans un déploiement passif ou en ligne (mode TAP), car le périphérique n'inspecte pas directement le trafic. Si vous créez une règle avec l'action **Bloquer** ou **Bloquer avec réinitialisation** qui contient des interfaces passives ou en ligne (mode TAP) dans une condition de zone de sécurité, l'éditeur de politique affiche un avertissement (⚠) à côté de la règle.

Actions de déchiffrement de Règle de déchiffrement

Les actions **Déchiffrer – Clé connue** et **Déchiffrer – Resigner** déchiffrent le trafic crypté. Le système inspecte le trafic déchiffré à l'aide du contrôle d'accès. Les règles de contrôle d'accès gèrent le trafic déchiffré et non chiffré de manière identique : vous pouvez les inspecter pour détecter des données de découverte, ainsi que détecter et bloquer les intrusions, les fichiers interdits et les programmes malveillants. Le système rechiffre le trafic autorisé avant de le transmettre à sa destination.

Nous vous recommandons d'utiliser un certificat provenant d'une autorité de certification (CA) de confiance pour déchiffrer le trafic. Cela empêche **Invalid Issuer** de s'afficher dans la colonne SSL Certificate Status dans les événements de connexion.

Pour plus d'informations sur l'ajout d'objets de confiance, consultez Objets autorité de certification approuvée.

Sujet connexe: : Bonnes pratiques de déchiffrement TLS 1.3

Sujets connexes

Bonnes pratiques de déchiffrement TLS 1.3

Surveiller l'accélération matérielle TLS/SSL

Les rubriques suivantes traitent de la surveillance de l'état de TLS/SSL

Compteurs informatifs

Si le système en charge fonctionne bien, les compteurs suivants devraient être nombreux. Étant donné que le processus de suivi comporte deux côtés par connexion, vous pouvez constater que ces compteurs augmentent de 2 par connexion. Les compteurs PRIV_KEY_RECV et SECU_PARAM_RECV sont les plus importants et sont mis en évidence. Les compteurs CONTEXT_CREATED et CONTEXT_DESTROYED se rapportent à l'allocation de la mémoire des puces de chiffrement.

```
> show counters
Protocol     Counter                        Value   Context
SSLENC       CONTEXT_CREATED               258225   Summary
SSLENC       CONTEXT_DESTROYED             258225   Summary
TLS_TRK      OPEN_SERVER_SESSION           258225   Summary
TLS_TRK      OPEN_CLIENT_SESSION           258225   Summary
TLS_TRK      UPSTREAM_CLOSE                516450   Summary
TLS_TRK      DOWNSTREAM_CLOSE              516450   Summary
TLS_TRK      FREE_SESSION                  516450   Summary
TLS_TRK      CACHE_FREE                    516450   Summary
TLS_TRK      PRIV_KEY_RECV                 258225   Summary
TLS_TRK      NO_KEY_ENABLE                 258225   Summary
TLS_TRK      SECU_PARAM_RECV               516446   Summary
```

```
TLS_TRK      DECRYPTED_ALERT                 258222   Summary
TLS_TRK      DECRYPTED_APPLICATION         33568976   Summary
TLS_TRK      ALERT_RX_CNT                    258222   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT          258222   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY           258222   Summary
TCP_PRX      OPEN_SESSION                    516450   Summary
TCP_PRX      FREE_SESSION                    516450   Summary
TCP_PRX      UPSTREAM_CLOSE                  516450   Summary
TCP_PRX      DOWNSTREAM_CLOSE                516450   Summary
TCP_PRX      FREE_CONN                       258222   Summary
TCP_PRX      SERVER_CLEAN_UP                 258222   Summary
TCP_PRX      CLIENT_CLEAN_UP                 258222   Summary
```

Compteurs d'alertes

Nous avons mis en place les compteurs suivants conformément à la spécification TLS 1.2. Les alertes FATAL ou BAD peuvent indiquer des problèmes; cependant, ALERT_RX_CLOSE_NOTIFY est normal

Pour plus de détails, consultez la section 7.2 de la RFC 5246.

```
TLS_TRK      ALERT_RX_CNT                      311   Summary
TLS_TRK      ALERT_TX_CNT                        2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT           2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT           2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT            308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY             308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC             2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC             2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE            1   Summary
```

Compteurs d'erreurs

Ces compteurs indiquent les erreurs du système. Dans un système sain, ces chiffres devraient être faibles. Les compteurs BY_PASS indiquent les paquets qui ont été transmis directement vers ou depuis le processus du moteur d'inspection (Snort) (qui s'exécute dans le logiciel) sans déchiffrement. L'exemple suivant énumère certains des compteurs défectueux.

Les compteurs ayant une valeur de 0 ne sont pas affichés. Pour afficher une liste complète des compteurs, utilisez la commande **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                         Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM            2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET          2   Summary
TLS_TRK      ENC_FAIL                           82   Summary
TLS_TRK      DEC_FAIL                          211   Summary
TLS_TRK      DEC_CKE_FAIL                    43194   Summary
TLS_TRK      ENC_CB_FAIL                      4335   Summary
TLS_TRK      DEC_CB_FAIL                       909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                   818   Summary
TLS_TRK      RECORD_PARSE_ERR                  123   Summary
TLS_TRK      IN_ERROR                        44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD           43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE              123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR          123   Summary
TLS_TRK      DECRYPT_FAIL                    43194   Summary
```

```
TLS_TRK      UPSTREAM_BY_PASS                  127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                127   Summary
```

Compteurs de pannes majeures

Les compteurs « fatal » indiquent des erreurs graves. Sur un système sain, ces compteurs devraient être égaux ou proches de 0. L'exemple suivant répertorie les compteurs « fatal »

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

Le compteur RING_FULL n'est pas un compteur fatal, mais indique combien de fois le système a surchargé la puce de chiffrement. Le compteur ACCELERATOR_RESET correspond au nombre de fois où le processus Accélération cryptographique TLS a échoué de manière inattendue. Cela entraîne également l'échec des opérations en cours, qui sont les chiffres que vous voyez dans ACCELERATOR_CORE_TIMEOUT et RSA_PRIVATE_DECRYPT_FAILED.

Si les problèmes persistent, désactivez Accélération cryptographique TLS (ou **config hwCrypto disable**) et collaborez avec Cisco TAC pour résoudre les problèmes.

Remarque Vous pouvez effectuer un dépannage supplémentaire en utilisant les commandes **show snort tls-offload** et **debug snort tls-offload**. Utilisez la commande **clear snort tls-offload** pour remettre à zéro les compteurs affichés dans la commande **show snort tls-offload**.

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.