



Renseignements de sécurité

Les rubriques suivantes fournissent un aperçu de Security Intelligence, y compris l'utilisation des listes de blocage et d'autorisation du trafic, ainsi que la configuration de base.

- [À propos des renseignements sur la sécurité, à la page 1](#)
- [Bonnes pratiques en matière de renseignements sur la sécurité, à la page 2](#)
- [Exigences de licence pour les renseignements sur la sécurité, à la page 3](#)
- [Exigences et conditions préalables pour les renseignements sur la sécurité, à la page 3](#)
- [Sources de renseignements sur la sécurité Security Intelligence, à la page 3](#)
- [Configurer les renseignements sur la sécurité, à la page 4](#)
- [Surveillance des renseignements sur la sécurité, à la page 12](#)
- [Remplacer le blocage des renseignements sur la sécurité, à la page 12](#)
- [Dépannage des renseignements sur la sécurité \(Security Intelligence\), à la page 13](#)

À propos des renseignements sur la sécurité

En tant que première ligne de défense contre le contenu malveillant, Security Intelligence utilise des renseignements sur la réputation pour bloquer rapidement les connexions vers ou à partir des adresses IP, des URL et des noms de domaine. C'est ce qu'on appelle *la liste de blocage Security Intelligence*.

Les renseignements sur la sécurité constituent une phase précoce du contrôle d'accès, avant que le système n'effectue des évaluations, qui consomment davantage de ressources. L'utilisation d'une liste de blocage améliore les performances en excluant rapidement le trafic qui ne nécessite pas d'inspection.



Remarque

Vous ne pouvez pas utiliser une liste de blocage pour bloquer le trafic accéléré. L'évaluation du préfiltre a lieu avant le filtrage Security Intelligence. Le trafic en acheminement rapide Fastpath contourne toute évaluation plus poussée, y compris Security Intelligence.

Bien que vous puissiez configurer des listes de blocage personnalisées, Cisco vous permet d'accéder à des flux de renseignements régulièrement mis à jour. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées.

Vous pouvez affiner la liste de blocage Security Intelligence à l'aide des listes Ne pas bloquer et des listes de blocage pour la surveillance uniquement. Ces mécanismes empêchent le trafic d'être bloqué par une liste de blocage, mais ne font **pas** automatiquement confiance au trafic correspondant ou ne lui offrent pas de voie

rapide. Le trafic ajouté à une liste Ne pas bloquer ou de surveillance à l'étape des renseignements sur la sécurité est délibérément soumis à une analyse plus approfondie avec le reste du contrôle d'accès.

Sujets connexes

[Renseignements de sécurité](#)

Bonnes pratiques en matière de renseignements sur la sécurité

- Configurez vos politiques de contrôle d'accès pour bloquer les menaces détectées par les flux de renseignements sur la sécurité fournis par Cisco. Consultez [Exemple de configuration : blocage du fait de renseignements sur la sécurité, à la page 10](#).
- Si vous souhaitez compléter les flux de Security Intelligence fournis par Cisco par des données sur les menaces personnalisées ou bloquer manuellement les menaces émergentes :
 - Pour les adresses IP, utilisez des listes et des flux de renseignements sur la sécurité personnalisés, ou des objets ou groupes réseau. Pour les créer, consultez [Renseignements de sécurité](#) et [Réseaut](#) leurs sujets secondaires. Pour les utiliser pour Security Intelligence, consultez [Configurer les renseignements sur la sécurité, à la page 4](#). Les objets réseau utilisés dans la politique de renseignement sur la sécurité nécessitent une licence IPS .
 - Pour les URL et les domaines, utilisez des listes et des flux de Security Intelligence personnalisés, et *non* des objets ou des groupes. Pour en savoir plus, reportez-vous à [Options de filtrage manuel d'URL](#)
 - Vous pouvez également ajouter des entrées à une liste de blocage à partir d'événements. Consultez [Listes des renseignements sur la sécurité globale et de domaine](#).
- Pour tester de nouveaux flux ou pour des déploiements passifs, définissez l'action de Block (Bloquer) à Surveiller uniquement. Consultez [Surveillance des renseignements sur la sécurité, à la page 12](#).
- Si vous devez exclure des sites ou des adresses spécifiques du blocage Security Intelligence, consultez [Remplacer le blocage des renseignements sur la sécurité, à la page 12](#).
- Si votre déploiement Firepower est intégré à SecureX ou à l'outil connexe Réponse aux menaces SecureX (anciennement Cisco Threat Response ou CTR) et que vous utilisez des listes et des flux de renseignements sur la sécurité personnalisés, veillez à mettre à jour l'échange des services de sécurité avec ces listes et ces flux. Pour en savoir plus, consultez les instructions de configuration de la promotion automatique des événements dans l'aide en ligne d'Exchange des services de sécurité.
- Les catégories de renseignements sur la sécurité fournies par le système peuvent changer avec le temps et sans avertissement. vous devez prévoir de vérifier périodiquement les changements et de modifier vos politiques en conséquence.
- Vous devez également configurer le filtrage d'URL, une fonctionnalité distincte ayant des exigences de licence distinctes, pour une protection accrue contre les sites malveillants. Consultez [Filtrage d'URL](#).

Exigences de licence pour les renseignements sur la sécurité

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les renseignements sur la sécurité

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau



Important

Vous devez appliquer la politique de découverte de réseau sur le périphérique pour une application réussie de la politique de Security Intelligence.

Sources de renseignements sur la sécurité Security Intelligence

- Flux de renseignements fournis par le système

Cisco fournit un accès à des flux de renseignements régulièrement mis à jour sur les domaines, les URL et les adresses IP. Pour en savoir plus, consultez [Renseignements de sécurité](#).

- Flux de tiers

Compléter les flux fournis par Cisco par des flux de réputation tiers, qui sont des listes dynamiques que Cisco Secure Firewall Management Center télécharge régulièrement d'Internet. Consultez [Flux de renseignements sur la sécurité personnalisés](#).

- Listes de blocage ou flux (ou objets ou groupes) personnalisés

Bloquez des adresses IP, des URL ou des noms de domaine spécifiques à l'aide d'une liste ou d'un flux créé manuellement (pour les adresses IP, vous pouvez également utiliser des objets ou des groupes de réseau.)

Par exemple, si vous avez connaissance d'adresses ou de sites malveillants qui ne sont pas encore bloqués par un flux, ajoutez ces sites à une liste de renseignements sur la sécurité personnalisée et ajoutez cette liste personnalisée à la liste de blocage dans l'onglet Security Intelligence de votre politique de contrôle d'accès, comme décrit dans [Listes de renseignements sur la sécurité personnalisés](#) et [Configurer les renseignements sur la sécurité](#), à la page 4.

Pour les adresses IP, vous pouvez éventuellement utiliser des objets de réseau plutôt que des listes ou des flux à cette fin; pour en savoir plus, consultez [Réseau](#). (Pour les URL, l'utilisation de listes et de flux est fortement recommandée plutôt que d'autres méthodes.)

- Listes ou flux personnalisés Ne pas bloquer

Remplacer le blocage des renseignements sur la sécurité pour des sites ou des adresses spécifiques. Consultez [Remplacer le blocage des renseignements sur la sécurité](#), à la page 12.

- Listes de blocage globales (une pour le réseau, l'URL et le DNS)

Lors de l'examen des événements, vous pouvez ajouter immédiatement l'adresse IP, l'URL ou le domaine d'un événement à la liste de blocage globale applicable afin que Security Intelligence gère le trafic futur provenant de cette source. Consultez [Listes des renseignements sur la sécurité globale et de domaine](#).

- Listes globales Ne pas bloquer (une pour le réseau, l'URL et le DNS)

Lors de l'examen des événements, vous pouvez ajouter immédiatement l'adresse IP, l'URL ou le domaine d'un événement à la liste globale des périphériques à Ne pas bloquer si vous ne voulez pas que Security Intelligence bloque le trafic futur provenant de cette source. Consultez [Listes des renseignements sur la sécurité globale et de domaine](#).

Configurer les renseignements sur la sécurité

Chaque politique de contrôle d'accès comporte des options de renseignement sur la sécurité. Vous pouvez ajouter des objets réseau, des objets et des listes d'URL, des flux et des listes de Security Intelligence à une liste de blocage ou une liste Ne pas bloquer, et les restreindre par zone de sécurité. Vous pouvez également associer une politique DNS à votre politique de contrôle d'accès et ajouter des noms de domaine à une liste de domaines à bloquer ou à ne pas bloquer.

Le nombre d'objets dans les listes Ne pas bloquer plus le nombre dans les listes de blocage ne peut pas dépasser 125 objets réseau ou 32 767 objets et listes d'URL.



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.

Avant de commencer

- Remarque : pour des conseils sur les recommandations de configuration minimale, consultez également [Exemple de configuration : blocage du fait de renseignements sur la sécurité, à la page 10](#).
- Pour vous assurer que toutes les options sont disponibles à la sélection, ajoutez au moins un périphérique géré à votre centre de gestion.
- Dans les déploiements passifs, ou si vous souhaitez définir le filtrage Security Intelligence comme « surveillance uniquement », activez la journalisation
- Configurez une politique DNS pour prendre des mesures de sécurité pour les domaines. Pour en savoir plus, consultez [Politiques DNS](#).

Procédure


- Étape 1** Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Security Intelligence** (Renseignements sur la sécurité).
- Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.
- Étape 2** Vous avez les options suivantes :
- Cliquez sur **Networks** (réseaux) pour ajouter des objets réseau (adresses IP).
Remarque Les objets réseau utilisés dans une politique de renseignement sur la sécurité nécessitent une licence IPS .
 - Cliquez sur **URLs** pour ajouter des objets URL.
- Étape 3** Recherchez les **objets disponibles** que vous souhaitez ajouter à la liste Bloquer ou Ne pas bloquer. Vous avez les options suivantes :
- Recherchez les objets disponibles en tapant dans le champ **Search by Name or value** (Rechercher par nom ou par valeur). Effacez la chaîne de caractères de recherche en cliquant sur **Recharger** (↻) ou **Effacer** (✕).
 - Si aucune liste ou aucun flux ne répond à vos besoins, cliquez sur **Ajouter** (+), sélectionnez **New Network List** (Nouvelle liste de réseaux) ou **New URL List** (Nouvelle liste d'URL), puis procédez comme décrit dans [Création de flux de renseignements sur la sécurité](#) ou [Téléversement de nouvelles listes de renseignements sur la sécurité vers Cisco Secure Firewall Management Center](#).
 - Si aucun objet existant ne répond à vos besoins, cliquez sur **Ajouter** (+), sélectionnez **New Network Object** (Nouvel objet réseau) ou **New URL Object** (Nouvel objet URL) et procédez comme décrit dans [Création d'objets réseau](#).
- Security Intelligence ignore les blocs d'adresses IP utilisant un masque de réseau /0.
- Étape 4** Choisissez un ou plusieurs **objets disponibles** à ajouter.
- Étape 5** (Facultatif) Choisissez une **zone disponible** pour restreindre les objets sélectionnés par zone.

Vous ne pouvez pas restreindre les listes de Security Intelligence fournies par le système par zone.

Remarque La zone **Any** (toute) pour une liste SI ne s'applique qu'aux interfaces qui font partie d'une zone de sécurité. Cependant, une exception est que si un périphérique n'a aucune interface associée à une zone de sécurité, la zone **Any** correspondra à n'importe quelle interface.

Par exemple, si vous avez cinq interfaces sur un périphérique et qu'aucune d'entre elles n'est associée à une zone de sécurité, toute liste Security Intelligence attribuée à la zone **Any** sera comparée au trafic sur TOUTES les interfaces du périphérique. Si vous ajoutez une interface à une zone de sécurité sur ce périphérique, cela supprimera efficacement l'inspection de Security Intelligence sur les quatre autres interfaces, où la zone est définie à **Any** pour une liste de Security Intelligence. Si vous ajoutez les quatre autres interfaces à une zone de sécurité, elles seront évaluées par la liste SI associée à la zone **Any**.

Étape 6 Cliquez sur **Ajouter à la liste Ne pas bloquer** ou sur **Ajouter à la liste de blocage**, ou cliquez sur les objets sélectionnés et faites-les glisser vers l'une ou l'autre de ces listes.

Pour supprimer un objet d'une liste de blocage ou Ne pas bloquer, cliquez sur **Supprimer** (). Pour supprimer plusieurs objets, choisissez les objets et effectuez un clic droit sur **Supprimer la sélection**.

Étape 7 (Facultatif) Définissez les objets de la liste de blocage pour qu'ils soient surveillés uniquement en effectuant un clic droit sur l'objet dans la **liste de blocage**, puis en sélectionnant **Monitor-only (do not block)** (Surveiller uniquement (ne pas bloquer)).

Vous ne pouvez pas définir les listes de renseignements sur la sécurité globales fournies par le système pour qu'elles soient « surveiller uniquement ».

Étape 8 Choisissez une politique DNS dans la liste déroulante **DNS Policy** (Politique DNS).

Étape 9 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

- [Renseignements de sécurité](#)
- [Scénarios de redémarrage de Snort](#)

Options de renseignements sur la sécurité

Utilisez l'onglet Security Intelligence (Renseignements sur la sécurité) dans l'éditeur de politique de contrôle d'accès pour configurer le réseau (adresse IP) et l'URL Security Intelligence, et pour associer la politique de contrôle d'accès à une politique DNS dans laquelle vous avez configuré Security Intelligence pour les domaines.

Objets disponibles

Les objets disponibles comprennent :

- Les catégories de renseignements sur la sécurité alimentées par le flux fourni par le système.

Pour de plus amples renseignements, consultez la section [Catégorie de renseignements sur la sécurité, à la page 8](#).

- Les listes de blocage global et Ne pas bloquer fournies par le système.

Pour une description, consultez [Sources de renseignements sur la sécurité Security Intelligence, à la page 3](#).

- Les listes et les flux de renseignements sur la sécurité que vous créez sous Objet > Gestion des objets > Security Intelligence.

Pour une description, consultez [Sources de renseignements sur la sécurité Security Intelligence, à la page 3](#).

- Les objets et groupes de réseau et d'URL configurés dans les pages respectives sous Objet > Gestion des objets. Ils sont différents des objets Security Intelligence du point précédent.

Pour en savoir plus sur les objets réseau, consultez [Réseau](#). (Pour les URL, utilisez des listes ou des flux de Security Intelligence plutôt que des objets ou des groupes.)

Zones disponibles

À l'exception des listes globales fournies par le système, vous pouvez restreindre le filtrage des renseignements sur la sécurité par zone.

Par exemple : pour améliorer les performances, vous pouvez cibler l'application. Comme exemple plus spécifique, vous pouvez bloquer les pourriels uniquement pour une zone de sécurité qui gère le trafic de messagerie.

Pour appliquer le filtrage Security Intelligence pour un objet sur plusieurs zones, vous devez ajouter l'objet à la liste Bloquer ou Ne pas bloquer séparément pour chaque zone.

Politique DNS

Afin de faire correspondre le trafic DNS à l'aide de Security Intelligence, vous devez sélectionner une politique DNS pour votre configuration Security Intelligence.

L'utilisation de listes de blocage ou Ne pas bloquer ou la surveillance du trafic en fonction d'une liste ou d'un flux DNS nécessite également de :

- Configurer les listes et les flux de DNS Security Intelligence. Consultez [Renseignements de sécurité](#).
- Créer une politique DNS. Consultez [Création de politiques DNS de base](#) pour obtenir de plus amples renseignements.
- Configurer des règles DNS qui font référence à vos listes ou à vos flux DNS. Consultez [Création et modification des règles DNS](#) pour obtenir de plus amples renseignements.
- Comme vous déployez la politique DNS dans le cadre de votre politique de contrôle d'accès, vous devez associer les deux politiques. Consultez [Déploiement de politique DNS](#) pour obtenir de plus amples renseignements.

Liste Ne pas bloquer

Consultez [Remplacer le blocage des renseignements sur la sécurité, à la page 12](#).

Pour sélectionner tous les objets de la liste, effectuez un clic droit sur un objet.

Liste de blocage

Reportez-vous à [Exemple de configuration : blocage du fait de renseignements sur la sécurité](#), à la page 10 et les autres rubriques de ce chapitre.

Pour des explications sur les indicateurs visuels de la liste de blocage, consultez [Icônes de la liste de blocage](#), à la page 10.

Pour sélectionner tous les objets de la liste, effectuez un clic droit sur un objet.

Logging (journalisation)

La journalisation des renseignements sur la sécurité, activée par défaut, consigne toutes les connexions bloquées et surveillées gérées par les périphériques cibles d'une politique de contrôle d'accès. Cependant, le système ne consigne pas les correspondances de la liste à ne pas bloquer; l'enregistrement des connexions sur la liste Ne pas bloquer dépend de leur disposition éventuelle. La journalisation doit être activée pour les connexions sur la liste de blocage avant que vous puissiez définir des objets de cette liste pour les surveiller uniquement.

Pour activer, désactiver ou afficher les paramètres de journalisation, effectuez un clic droit sur un objet dans la liste de blocage.

Sujets connexes

- [Listes des renseignements sur la sécurité globale et de domaine](#)
- [Listes d'informations de sécurité et multilocalisation de détention](#)

Catégorie de renseignements sur la sécurité

Les catégories de renseignements sur la sécurité sont déterminées par les flux fournis par le système, décrits dans [Renseignements de sécurité](#).

Ces catégories sont utilisées aux emplacements suivants :

- Le sous-onglet Networks (réseaux) de l'onglet Security Intelligence d'une politique de contrôle d'accès
- Le sous-onglet URL à côté de l'onglet Networks (réseaux) dans l'onglet Security Intelligence d'une politique de contrôle d'accès
- Dans une politique DNS, sur l'onglet DNS de la page de configuration des règles DNS
- Dans les événements générés lorsque le trafic correspond aux configurations de blocage ou de surveillance dans les emplacements ci-dessus

**Remarque**

Si votre entreprise utilise Directeur de Cisco Secure Firewall threat intelligence : lors de l'affichage des événements, vous pouvez voir des catégories indiquant que l'action a été entreprise par TID, comme TID URL Block (blocage d'URL TID).

Les catégories sont mises à jour par Talos à partir du nuage, et cette liste peut changer indépendamment des versions de Firepower.

Tableau 1 : Catégories de flux Cisco Talos Intelligence Group (Talos)

Catégorie de renseignements sur la sécurité	Description
Agresseurs	Analyseurs et hôtes actifs connus pour les activités malveillantes sortantes
fraude_bancaire	Sites qui se livrent à des activités frauduleuses liées aux services bancaires électroniques
bogon	Réseaux de bogons et adresses IP non attribuées
Robots logiciels	Sites qui hébergent des pipettes de programmes malveillants binaires
CNC	Sites qui hébergent des serveurs de commande et de contrôle pour les réseaux de zombies
Cryptominage	Hôtes fournissant un accès à distance aux ensembles et aux portefeuilles dans le but d'exploiter des crypto-devises
Dga	Algorithmes de programmes malveillants utilisés pour générer un grand nombre de noms de domaine agissant comme points de rendez-vous avec leurs serveurs de commande et de contrôle
Kit d'exploit	Trousses de logiciels conçues pour identifier les vulnérabilités des logiciels des clients.
Risque_élevé	Les domaines et les noms d'hôte qui correspondent aux algorithmes de sécurité prédictive OpenDNS du graphique de sécurité
Ioc	Hôtes qui ont été observés en train de s'engager dans les indicateurs de compromission (IOC)
partage_de_liens	Sites Web qui partagent des fichiers protégés par des droits d'auteur sans autorisation
Malveillant	Sites ayant un comportement malveillant qui ne correspondent pas nécessairement à une autre catégorie de menace, plus précise,
Malicieux	Sites qui hébergent des fichiers binaires ou des kits d'exploit de programmes malveillants
Nouvellement_vu	Les domaines qui ont été récemment enregistrés ou qui ne sont pas encore vus par télémétrie. Attention Actuellement, cette catégorie ne comporte aucun flux actif et est réservée pour une utilisation future.
Mandataires_ouverts	Des mandataires ouverts qui permettent la navigation anonyme sur le Web
Relais_ouvert	Ouvrir les relais de messagerie connus pour être utilisés pour les pourriels
Hameçonnage	Les sites qui hébergent des pages d'hameçonnage

Catégorie de renseignements sur la sécurité	Description
Intervention	Adresses IP et URL qui participent activement à des activités malveillantes ou suspectes
Pourriels	Hôtes de messagerie connus pour envoyer des pourriels
Logiciel espion	Sites connus pour contenir, diffuser ou soutenir des activités de logiciels espions et publicitaires
Suspect	Fichiers qui semblent suspects et dont les caractéristiques ressemblent à celles d'un logiciel malveillant connu
nœud_exit_de_tor	Hôtes connus pour offrir des services de nœud de sortie pour le réseau d'anonymisation Tor

Icônes de la liste de blocage

Les indicateurs visuels suivants peuvent apparaître dans la liste de blocage de l'onglet Security Intelligence dans une politique de contrôle d'accès :

Icône ou indicateur visuel	Description
Bloquer (🚫)	L'objet est défini sur Block (blocage).
Moniteur (👁️)	L'objet est défini comme surveillance uniquement. Voir la section Surveillance des renseignements sur la sécurité , à la page 12.
Un objet est affiché en texte barré	Le même objet se trouve également dans la liste Ne pas bloquer, qui remplace le blocage.

Exemple de configuration : blocage du fait de renseignements sur la sécurité

Configurez votre politique de contrôle d'accès pour bloquer toutes les menaces détectables par les flux de renseignements sur la sécurité régulièrement mis à jour du système.

Le nombre d'objets des listes de blocage plus le nombre d'objets des listes à ne pas bloquer ne peut pas dépasser 125 objets réseau ou 32 767 objets et listes d'URL.



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.

Avant de commencer

- Pour vous assurer que toutes les options sont disponibles à la sélection, ajoutez au moins un périphérique géré à votre centre de gestion.
- Configurer une politique DNS pour bloquer toutes les catégories de menaces de renseignements sur la sécurité pour les domaines. Pour en savoir plus, consultez [Politiques DNS](#).
- Si vous avez ou aurez des listes personnalisées d'entités à bloquer, créez un objet de renseignement sur la sécurité de chaque type (URL, DNS, réseaux.) Consultez [Renseignements de sécurité](#).

Procédure

- Étape 1** Cliquez sur **Policies (politiques) > Access Control (contrôle d'accès)**.
- Étape 2** Créez une nouvelle politique de contrôle d'accès ou modifiez une politique existante.
- Étape 3** Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Security Intelligence** (Renseignements sur la sécurité).
- Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.
- Étape 4** Cliquez sur **Networks (réseaux)** pour ajouter des critères de blocage pour les adresses IP.
- Faites défiler la liste des réseaux vers le bas et sélectionnez toutes les catégories de menaces répertoriées sous les listes globales.
 - Le cas échéant, sélectionnez les zones de sécurité pour lesquelles vous souhaitez bloquer ces menaces.
 - Cliquez sur **Add to Block List** (Ajouter à la liste de blocage).
 - Si vous avez créé des listes ou des flux personnalisés avec des adresses à bloquer, ajoutez-les à la liste de blocage en utilisant les mêmes étapes que ci-dessus.
- Étape 5** Cliquez sur **URL** pour ajouter des critères de blocage pour les URL et répétez les étapes que vous avez suivies pour les réseaux.
- Étape 6** Choisissez une politique DNS dans la liste déroulante **DNS Policy** (Politique DNS); voir [Aperçu de la politique DNS](#).
- Étape 7** Cliquez sur **Save** (enregistrer).
-

Prochaine étape

- Activer la journalisation pour ces connexions
- Déployer les changements de configuration.
- Pour une protection supplémentaire, configurez le filtrage d'URL pour bloquer les URL malveillantes. Consultez [Filtrage d'URL](#).

Surveillance des renseignements sur la sécurité

La surveillance journalise les événements de connexion pour le trafic qui aurait été bloqué par Security Intelligence, mais ne bloque pas le trafic. La surveillance est particulièrement utile pour :

- tester les flux avant de les mettre en œuvre;

Voici un scénario dans lequel vous souhaitez tester un flux tiers avant de mettre en œuvre le blocage à l'aide de ce flux. Lorsque vous réglez le flux comme « surveillance uniquement », le système permet au système d'analyser plus avant les connexions qui auraient été bloquées, mais il enregistre également un enregistrement de chacune de ces connexions pour votre évaluation.

- Déploiements passifs, pour optimiser les performances.

Les périphériques gérés qui sont déployés de manière passive ne peuvent pas affecter le flux de trafic; il n'y a aucun avantage à configurer le système pour bloquer le trafic. En outre, étant donné que les connexions bloquées ne sont pas réellement bloquées dans les déploiements passifs, le système peut signaler plusieurs événements de début de connexion pour chaque connexion bloquée.



Remarque

S'il est configuré, Directeur de Cisco Secure Firewall threat intelligence peut avoir une incidence sur l'action prise (Surveiller ou Bloquer).

Pour configurer la surveillance Security Intelligence :

Après avoir configuré le blocage Security Intelligence en suivant les instructions dans [Exemple de configuration : blocage du fait de renseignements sur la sécurité, à la page 10](#), effectuez un clic droit sur chaque objet applicable dans la liste de blocage et sélectionnez **Monitor-only** (Surveiller uniquement). Vous ne pouvez pas définir les listes de Security Intelligence fournies par le système pour qu'elles soient de type « Surveiller uniquement ».

Remplacer le blocage des renseignements sur la sécurité

Vous pouvez également utiliser les listes de ne pas bloquer pour éviter que des domaines, des URL ou des adresses IP spécifiques ne soient bloqués par les listes ou les flux de Security Intelligence.

Par exemple, vous pouvez :

- Remplacer le blocage occasionnel de faux positifs dans un flux de renseignements sur la sécurité réputé
- Inspecter un trafic spécifique en profondeur au lieu de le bloquer précocement en fonction de la réputation
- Exempter les transactions par ailleurs restreintes en fonction de la zone du blocage des services Security Intelligence

Par exemple, vous pouvez ajouter une URL mal classée à une liste à ne pas bloquer, mais ensuite restreindre l'objet de liste à ne pas bloquer en utilisant une zone de sécurité utilisée par les membres de votre organisation qui doivent accéder à ces URL. De cette façon, seules les personnes ayant des besoins commerciaux peuvent accéder aux URL de la liste Ne pas bloquer.

**Remarque**

Les entrées sur une liste de blocage sont simplement des exceptions de la liste de blocage. Toute connexion qui réussit la politique de renseignements sur la sécurité est soumise aux règles de contrôle d'accès. Ainsi, une entrée de la liste Ne pas bloquer peut par la suite être bloquée par une règle de contrôle d'accès ou une politique de prévention des intrusions. Vos entrées Ne pas bloquer doivent toujours être des exceptions à vos listes de blocage.

Procédure**Étape 1**

Option 1 : ajouter une adresse IP, une URL ou un domaine d'un événement à la liste globale des périphériques non bloqués. Consultez [Listes des renseignements sur la sécurité globale et de domaine](#).

Étape 2

Option 2 : Utiliser une liste ou un flux de renseignements sur la sécurité personnalisé

- a) Créez la liste ou le flux de renseignements sur la sécurité personnalisé. Reportez-vous aux sections [Listes de renseignements sur la sécurité personnalisés](#) ou [Création de flux de renseignements sur la sécurité](#).
- b) Pour les adresses IP (réseaux) et les URL : modifiez votre politique de contrôle d'accès, cliquez sur l'onglet Security Intelligence, cliquez sur la liste ou le flux personnalisé dans le sous-onglet Networks or URLs , puis cliquez sur **Add to Do Not Block List**.
- c) Enregistrez vos modifications.
- d) Pour les domaines (DNS) : consultez la section « Politique DNS » dans la rubrique [Options de renseignements sur la sécurité, à la page 6](#).
- e) Déployez vos modifications.

Dépannage des renseignements sur la sécurité (Security Intelligence)

Consultez les rubriques suivantes pour le dépannage des renseignements sur la sécurité.

Des catégories de renseignements sur la sécurité sont manquantes dans la liste des options disponibles

Symptômes : Sous l'onglet Security Intelligence de la politique de contrôle d'accès, les catégories Security Intelligence (comme CnC ou Exploit Kit) ne s'affichent pas dans l'onglet Networks (Réseaux) sous les options disponibles.

Cause :

- Ces catégories ne s'affichent pas tant que vous n'avez pas ajouté au moins un périphérique géré à votre centre de gestion. Vous devez ajouter un périphérique pour pouvoir extraire tous les flux TALOS.
- La fonctionnalité de filtrage d'URL utilise un ensemble de catégories différent de celui de la fonctionnalité Security Intelligence; la catégorie que vous vous attendez à voir est peut-être une catégorie de filtrage d'URL. Pour voir les catégories de filtrage d'URL, consultez l'onglet **URL** dans une règle de contrôle d'accès.

Des catégories de renseignements sur la sécurité sont manquantes dans la liste des options disponibles

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.