Contrôle d'accès

Les rubriques suivantes expliquent comment gérer les règles de contrôle d'accès. Ces règles contrôlent le trafic autorisé à passer par le périphérique et appliquent des services avancés au trafic, comme l'inspection de prévention des intrusions.

Bonnes pratiques pour les règles de contrôle d'accès

La politique de contrôle d'accès est votre outil principal pour protéger vos réseaux internes et empêcher vos utilisateurs d'accéder à des ressources de réseau externes indésirables, comme les sites Web inappropriés. Ainsi, nous vous recommandons d'accorder une attention particulière à cette politique et de l'affiner pour obtenir le niveau de protection et de connectivité dont vous avez besoin.

La procédure suivante fournit un aperçu des éléments de base que vous devez faire avec la politique de contrôle d'accès. Il s'agit d'un aperçu et ne fournit pas d'étapes exhaustives pour effectuer chaque tâche.

Pour accéder à la politique de contrôle d'accès, choisissez **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.

Procédure

Étape 1 Configurez l'action par défaut pour la politique.

L'action par défaut gère les connexions qui ne correspondent pas aux règles spécifiques de la politique. Par défaut, cette action est **Block** (Bloquer), de sorte que tout ce que vous manquez dans les règles est bloqué. Ainsi, il vous suffit d'écrire des règles de contrôle d'accès qui autorisent le trafic souhaité. Il s'agit de la façon traditionnelle de configurer la politique de contrôle d'accès.

Vous pouvez faire le contraire, où vous autorisez le trafic par défaut et écrivez des règles qui suppriment le trafic indésirable connu, de sorte que vous n'avez pas besoin d'avoir des règles pour tout ce que vous souhaitez

autoriser. Cela facilite l'utilisation des nouveaux services, mais ouvre le risque que le nouveau trafic indésirable passe avant que vous ne le remarquiez.

Étape 2 Cliquez sur le bouton **Access Policy Settings** (Paramètres de la politique d'accès) ( ) et activez l'option **TLS Server Identity Discovery**.

Cette option améliore la détection initiale de l'application et l'identification de la catégorie d'URL et de la réputation pour les connexions TLS 1.3. Si vous n'activez pas cette option, le trafic TLS 1.3 pourrait ne pas correspondre aux règles que vous souhaitez. Cette option peut également améliorer l'efficacité des règles de déchiffrement.

Étape 3 Créez aussi peu de règles de contrôle d'accès que possible.

Avec les pare-feu traditionnels, vous pourriez vous retrouver avec des dizaines de milliers de règles pour diverses combinaisons d'adresse IP et de port. Avec un pare-feu de nouvelle génération, vous pouvez utiliser l'inspection avancée et éviter certaines de ces règles détaillées. Moins vous avez de règles, plus rapide le système peut évaluer le trafic et plus il sera facile pour vous de détecter et de résoudre les problèmes dans votre ensemble de règles.

Étape 4 Activation de la journalisation pour vos règles de contrôle d'accès.

Les statistiques sont collectées pour le trafic correspondant uniquement si vous activez la journalisation. Vos tableaux de bord de surveillance seront inexacts si vous n'activez pas la journalisation.

Étape 5 Placez des règles très spécifiques en haut de la politique, et assurez-vous que les règles spécifiques sont supérieures à toute règle plus générale qui correspondrait aux connexions auxquelles une règle spécifique correspondrait également.

La politique est évaluée de haut en bas, la première correspondance l'emporte. Ainsi, si vous mettez dans une règle qui bloque tout le trafic vers un sous-réseau spécifique, puis suivez-la avec une règle qui permet l'accès à une adresse IP unique dans le sous-réseau, le trafic vers cette adresse ne sera pas autorisé, car la première règle le bloquera.

En outre, placez des règles qui ciblent le trafic en fonction uniquement des critères classiques, tels que l'interface d'entrée/sortie, l'adresse IP source/destination, le port ou la géolocalisation, avant les règles qui nécessitent une inspection approfondie, comme celles qui s'appliquent aux critères de l'utilisateur, au filtrage d'URL ou au filtrage d'application. Étant donné que ces règles ne nécessitent pas d'inspection, leur application précoce peut vous aider à prendre des décisions de contrôle d'accès plus rapides pour les connexions correspondantes.

Pour plus de suggestions, consultez Bonnes pratiques pour l'ordre des règles de contrôle d'accès, à la page 15.

Étape 6 Associez les règles de blocage et d'autorisation pour cibler des sous-ensembles de trafic.

Par exemple, il est possible que vous souhaitiez autoriser un volume important de trafic HTTP/HTTPS, tout en bloquant l'accès à certains sites indésirables, comme la pornographie ou les jeux d'argent. Vous pouvez le faire en créant les règles suivantes et en les gardant séquentielles dans la politique (par exemple, règles 11 et 12).

- Une règle de blocage de filtrage d'URL qui cible les catégories d'URL indésirables, appliquée à la zone de sécurité interne (source) et à la zone de sécurité externe (destination), et toute adresse IP, tout port ou géolocalisation. Par exemple, blocage des réseaux de zombies, contenu maltraitant envers les enfants, cryptojacking, tunnellisation DNS, fraude bancaire en ligne, exploits, évitement de filtre, jeux d'argent, piratage, discours de haine, sites et emplacements à haut risque, activités illégales, téléchargements illégaux, drogues illégales, sites malveillants, sites de programmes malveillants, menaces mobiles, nœud de programmes malveillants P2P, hameçonnage, pornographie, pourriels, logiciels espions et logiciels publicitaires.

- Une règle d'autorisation de filtrage d'application pour les applications HTTP et HTTPS, appliquée à la zone de sécurité interne (source) et à la zone de sécurité externe (destination), et toute adresse IP, tout port ou géolocalisation. Une fois que la règle de filtrage d'URL a bloqué l'accès aux ressources Web indésirables, cette règle autorise tous les autres accès HTTP/HTTPS.

Étape 7 Utilisez les fonctionnalités de pare-feu de nouvelle génération pour cibler le trafic, quels que soient l'adresse IP ou le port.

Les agresseurs ou d'autres personnes malveillantes peuvent fréquemment modifier les adresses IP et les ports pour contourner les critères de correspondance du trafic de contrôle d'accès traditionnel. Au lieu de cela, utilisez les fonctionnalités de nouvelle génération suivantes :

- Critères de l'utilisateur : configurez la politique d'identité pour obtenir des informations sur l'utilisateur qui lance le trafic. Idéalement, votre serveur Active Directory organise les utilisateurs en groupes, et vous pouvez créer des règles de contrôle d'accès qui autorisent ou bloquent le trafic en fonction de l'appartenance au groupe d'utilisateurs. Par exemple, autorisez les spécialistes en ingénierie à accéder à vos sous-réseaux de développement, mais bloquez implicitement toute personne qui ne fait pas partie du groupe des spécialistes en ingénierie. Utilisez des groupes plutôt que des noms d'utilisateurs individuels, de sorte que vous n'avez pas besoin de mettre à jour continuellement les règles à mesure que des personnes sont ajoutées au réseau.
- Critères d'application : utilisez les critères de filtrage d'application pour autoriser ou bloquer les types d'application. Ainsi, si un utilisateur modifie les ports pour une connexion HTTP, le système peut reconnaître qu'il s'agit d'une connexion HTTP, même s'il ne va pas au port 80. Pour plus de suggestions, consultez Bonnes pratiques pour le filtrage d'applications, à la page 6.
- Catégorie d'URL et critères de réputation : utilisez le filtrage d'URL basé sur la catégorie pour autoriser ou bloquer dynamiquement les sites en fonction du type de site. Dans le type ou la catégorie du site, vous pouvez affiner votre règle selon que le site a la réputation d'être bon ou mauvais acteur. En utilisant la catégorie et la réputation, vous n'aurez pas besoin d'ajuster constamment vos règles, car les sites changent d'URL, ce que vous devriez faire si vous avez essayé de bloquer manuellement les sites par URL. Pour plus de suggestions, consultez Bonnes pratiques pour un filtrage d'URL efficace, à la page 11.

  Vous pouvez également appliquer vos règles de catégorie et de réputation de filtrage d'URL aux demandes de consultation DNS. Le système peut empêcher la réponse DNS pour la catégorie bloquée/la réputation, bloquant efficacement la tentative de connexion de l'utilisateur. Pour de plus amples renseignements, consultez la section Filtrage des requêtes DNS en fonction de la catégorie d'URL et de la réputation, à la page 13.

Étape 8 Appliquez l'inspection des intrusions à toutes vos règles d'autorisation.

L'un des aspects les plus importants des pare-feu de nouvelle génération est que vous pouvez appliquer l'inspection des intrusions et le contrôle d'accès à l'aide du même périphérique. Appliquez une politique de prévention des intrusions à chaque règle d'autorisation, de sorte que si une attaque entre dans votre réseau par un chemin normalement inoffensif, vous puissiez la détecter et abandonner la connexion d'attaque.

Si votre action par défaut est Allow (autoriser), vous pouvez également appliquer une protection contre les intrusions pour le trafic qui correspond à l'action par défaut.

Étape 9 Configurez également la Security Intelligence policy (politique Security Intelligence) pour bloquer les adresses IP et les URL indésirables.

La politique Security Intelligence est appliquée avant la politique de contrôle d'accès, de sorte qu'elle peut bloquer les connexions indésirables avant que vos règles de contrôle d'accès ne soient même évaluées. Cela peut fournir un blocage précoce et vous aider à réduire la complexité de vos règles de contrôle d'accès.

Étape 10 Envisagez de mettre en œuvre la SSL Decryption policy (politique de déchiffrement SSL).

Le système n'effectue pas d'inspection approfondie du trafic chiffré. Si vous configurez la politique de déchiffrement SSL, la politique de contrôle d'accès est appliquée à une version déchiffrée du trafic. Ainsi, l'inspection approfondie peut identifier les attaques (à l'aide de la politique de prévention des intrusions) et la mise en correspondance des règles est meilleure, car le filtrage des applications et des URL peut être appliqué plus efficacement. Tout trafic autorisé par la politique de contrôle d'accès est ensuite rechiffré avant d'être envoyé par le périphérique, de sorte que l'utilisateur final ne perd pas la protection du chiffrement.

Étape 11 Activez la recherche de groupe d'objets pour simplifier le déploiement de vos règles.

L'activation de la recherche de groupe d'objets réduit les besoins en mémoire pour les stratégies de contrôle d'accès qui incluent des objets réseau. Cependant, il est important de noter que la recherche par groupe d'objets peut également diminuer les performances de la recherche de règles et donc augmenter l'utilisation de l'unité centrale. Vous devez équilibrer l'incidence sur le processeur et le besoin en mémoire réduits pour la stratégie de contrôle d'accès spécifique. Dans la plupart des cas, l'activation de la recherche de groupe d'objets offre une nette amélioration opérationnelle.

Vous pouvez définir cette option à l'aide de FlexConfig en envoyant la commande **object-group-search access-control** ; utilisez la forme **no** de la commande dans le modèle de négation.

Aperçu du contrôle d'accès

Les rubriques suivantes expliquent comment gérer les règles de contrôle d'accès.

Règles de contrôle d'accès et action par défaut

Utilisez la politique de contrôle d'accès pour autoriser ou bloquer l'accès aux ressources réseau. La politique consiste en un ensemble de règles ordonnées, qui sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic.

Vous pouvez contrôler l'accès en fonction des éléments suivants :

- Caractéristiques du réseau traditionnelles telles que les adresses IP source et de destination, le protocole, les ports et les interfaces (sous forme de zones de sécurité).
- Le nom de domaine complet (FQDN) de la source ou de la destination (sous forme d'objet réseau). La correspondance du trafic est basée sur l'adresse IP renvoyée pour le nom d'une recherche DNS.
- La balise de groupe de sécurité (SGT) attribuée à la source ou à la destination par le Cisco Identity Services Engine (ISE).
- L'application qui est utilisée. Vous pouvez contrôler l'accès en fonction de l'application spécifique ou vous pouvez créer des règles qui couvrent les catégories d'applications, les applications marquées d'une caractéristique particulière, le type d'application (client, serveur, Web) ou l'évaluation de risque ou de pertinence commerciale de l'application.
- L'URL de destination d'une demande Web, y compris la catégorie généralisée de l'URL. Vous pouvez affiner les correspondances de catégorie en fonction de la réputation publique du site cible.

- La catégorie d'URL et la réputation d'un FQDN dans une demande de recherche DNS. Vous pouvez bloquer la réponse DNS pour les catégories indésirables ou pour mauvaise réputation, ce qui empêche efficacement la tentative de connexion ultérieure.
- L'utilisateur qui fait la demande ou les groupes d'utilisateurs auxquels l'utilisateur appartient.

Pour le trafic non chiffré que vous autorisez, vous pouvez appliquer l'inspection IPS pour vérifier les menaces et bloquer le trafic qui semble être une attaque. Vous pouvez également utiliser des politiques de fichiers pour vérifier les fichiers interdits ou les programmes malveillants.

Tout trafic qui ne correspond à aucune règle de contrôle d'accès est géré par l'action par défaut de contrôle d'accès **Default Action** (Action par défaut). Si vous autorisez le trafic par défaut, vous pouvez appliquer l'inspection de prévention des intrusions au trafic. Cependant, vous ne pouvez pas inspecter les fichiers ou les programmes malveillants sur le trafic géré par l'action par défaut.

Filtrage d'applications

Vous pouvez utiliser des règles de contrôle d'accès pour filtrer le trafic en fonction de l'application utilisée dans la connexion. Le système peut reconnaître une grande variété d'applications, de sorte que vous n'avez pas besoin de comprendre comment bloquer une application Web sans bloquer toutes les applications Web.

Pour certaines applications populaires, vous pouvez filtrer selon différents aspects de l'application. Par exemple, vous pourriez créer une règle qui bloque les jeux Facebook sans bloquer tout Facebook.

Vous pouvez également créer des règles en fonction des caractéristiques générales des applications, en bloquant ou en autorisant des groupes entiers d'applications selon le risque ou la pertinence métier, le type, la catégorie ou la balise. **Toutefois, lorsque vous sélectionnez des catégories dans un filtre d'application, consultez la liste des applications correspondantes pour vous assurer de ne pas inclure d'applications non souhaitées.** Pour une explication détaillée des regroupements possibles, consultez Critères d'application, à la page 25.

Application Control pour le trafic chiffré et déchiffré

Si une application utilise le chiffrement, le système pourrait ne pas être en mesure d'identifier l'application.

Le système peut détecter le trafic d'applications chiffré avec StartTLS, y compris SMTPS, POPS, FTPS, TelnetS et IMAPS. En outre, il peut identifier certaines applications chiffrées en fonction de l'indication du nom du serveur dans le message TLS ClientHello ou de la valeur du nom distinctif du sujet provenant du certificat du serveur.

Utilisez la boîte de dialogue Application Filters (Filtres d'application) pour déterminer si votre application nécessite un déchiffrement : sélectionnez les Tags (Balises) suivants, puis examinez la liste des applications.

- **SSL Protocol** (Protocole SSL) : vous n'avez pas besoin de déchiffrer le trafic associé à la balise SSL Protocol. Le système peut reconnaître ce trafic et appliquer votre action de contrôle d'accès. Les règles de contrôle d'accès pour les applications répertoriées doivent correspondre aux connexions attendues.
- **Decrypted Traffic** (Trafic déchiffré) : le système ne peut reconnaître ce trafic que si vous le déchiffrez d'abord. Configurez des règles de déchiffrement SSL pour ce trafic.

Filtrage en fonction du protocole industriel commun (CIP) et des applications Modbus (ISA 3000)

Vous pouvez activer le protocole industriel commun (CIP) et les préprocesseurs Modbus sur les périphériques Cisco ISA 3000, et filtrer en fonction des applications CIP et Modbus dans les règles de contrôle d'accès.

Tous les noms d'applications CIP commencent par « CIP », tel que CIP Write. Il n'y a qu'une seule application pour Modbus.

Pour activer les préprocesseurs, vous devez passer en mode expert dans une session CLI (SSH ou console) et exécuter la commande suivante pour activer l'une ou les deux applications de contrôle de supervision et d'acquisition de données (SCADA).

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

Par exemple, pour activer les deux préprocesseurs :

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```

Remarque Vous devez exécuter cette commande après chaque déploiement. Ces préprocesseurs sont désactivés lors du déploiement.

Bonnes pratiques pour le filtrage d'applications

Veuillez garder les recommandations suivantes à l'esprit lors de la conception des règles de contrôle d'accès de filtrage d'application.

- Pour gérer le trafic référencé par un serveur Web, tel que le trafic publicitaire, faites correspondre l'application référencée plutôt que l'application de référence.
- Évitez de combiner les critères d'application et d'URL dans la même règle, en particulier pour le trafic chiffré.
- Si vous écrivez une règle pour un trafic étiqueté **Decrypted Traffic** (Trafic déchiffré), assurez-vous de disposer d'une règle SSL Decryption (Déchiffrement SSL) qui déchiffrera le trafic correspondant. Ces applications ne peuvent être identifiées que dans les connexions déchiffrées.
- TLS 1.3 chiffre la plupart des messages d'établissement de liaison, de sorte que les renseignements sur les certificats ne sont pas facilement accessibles. Pour que le trafic chiffré avec TLS 1.3 corresponde efficacement aux critères d'accès qui utilisent le filtrage d'applications ou d'URL, le système doit obtenir un certificat en clair pour le serveur. Nous vous recommandons d'activer **TLS 1.3 Certificate Visibility (visibilité des certificats TLS 1.3)** dans les paramètres de contrôle d'accès. Si vous activez cette option, le système vérifie si un certificat pour le site est stocké en cache en fonction de l'adresse IP et de l'indication du nom du serveur (SNI) dans le paquet client « hello » Si aucun certificat n'est disponible, le système utilise une sonde TLS 1.2 pour obtenir le certificat, qui pourra ensuite être utilisé pour identifier la catégorie et la réputation de l'application ou de l'URL sans déchiffrer la connexion.
- Le système peut détecter plusieurs types de trafic d'application Skype. Pour contrôler le trafic Skype, choisissez la balise Skype dans la liste Application Filters (Filtres d'application) plutôt que de sélectionner des applications individuelles. Cela garantit que le système peut détecter et contrôler tout le trafic de Skype de la même manière.
- Pour contrôler l'accès à la messagerie Zoho, sélectionnez les applications Zoho et Zoho Mail.

Filtrage URL

Vous pouvez utiliser des règles de contrôle d'accès pour filtrer le trafic en fonction de l'URL utilisée dans une connexion HTTP ou HTTPS. Notez que le filtrage d'URL pour HTTP est plus simple que pour HTTPS, car HTTPS est chiffré.

Vous pouvez utiliser les techniques suivantes pour mettre en œuvre le filtrage d'URL.

- Filtrage d'URL basé sur la catégorie et la réputation : avec une licence de filtrage d'URL, vous pouvez contrôler l'accès aux sites Web en fonction de la classification générale de l'URL (catégorie) et du niveau de risque (réputation). Il s'agit de loin du moyen le plus simple et le plus efficace pour bloquer les sites indésirables.
- Filtrage manuel d'URL : avec n'importe quelle licence, vous pouvez spécifier manuellement des URL individuelles et des groupes d'URL afin d'obtenir un contrôle granulaire et personnalisé du trafic Web. L'objectif principal du filtrage manuel est de créer des exceptions aux règles de blocage basées sur une catégorie, mais vous pouvez utiliser des règles manuelles à d'autres fins.

Les rubriques suivantes fournissent des informations supplémentaires sur le filtrage d'URL.

Filtrage des URL par catégorie et par réputation

Avec une licence de filtrage d'URL, vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie et de la réputation des URL demandées :

- Catégorie : classification générale pour l'URL. Par exemple, eBay.com appartient à la catégorie Enchères et monster.com appartient à la catégorie Recherche d'emploi. Une URL peut appartenir à plusieurs catégories.
- Réputation : la probabilité que l'URL soit utilisée à des fins contraires à la politique de sécurité de votre organisation. Les réputations vont de Les réputations s'échelonnent de Non fiable (niveau 1) à Fiable (niveau 5).

Les catégories d'URL et les réputations vous aident à configurer rapidement le filtrage d'URL. Par exemple, vous pouvez utiliser le contrôle d'accès pour bloquer les URL non fiables dans la catégorie Drogues illégales.

Pour une description des catégories, consultez https://www.talosintelligence.com/categories.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Des sites qui (par exemple) représentent des menaces pour la sécurité ou qui diffusent du contenu indésirable peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer de nouvelles politiques. Lorsque Cisco met à jour la base de données d'URL avec de nouveaux sites, des classifications modifiées et des réputations modifiées, vos règles s'ajustent automatiquement aux nouvelles informations. Vous n'avez pas besoin de modifier vos règles pour prendre en compte les nouveaux sites.

Si vous activez les mises à jour régulières de la base de données d'URL, vous pouvez vous assurer que le système utilise des informations à jour pour le filtrage d'URL. Vous pouvez également activer les communications avec Cisco Collective Security Intelligence (CSI) pour obtenir les dernières informations sur les menaces pour les URL de catégorie et de réputation inconnues. Pour en savoir plus, consultez Configuration des préférences de filtrage Cloud .

Remarque Pour voir les informations de catégorie d'URL et de réputation dans les événements et les détails de l'application, vous devez créer au moins une règle avec une condition d'URL.

Recherche de la catégorie et de la réputation d'une URL

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Vous pouvez accéder à l'onglet URL d'une règle de contrôle d'accès ou d'une règle de déchiffrement SSL, ou encore aller à **Device (Périphérique)** > **System Settings (Paramètres système)** > **URL Filtering Preferences (Préférences de filtrage d'URL)**. Vous pouvez y saisir l'URL dans le champ **URL to Check** (URL à vérifier) et cliquer sur **Go** (Aller).

Vous serez redirigé vers un site Web qui affiche les résultats de la recherche. Vous pouvez utiliser ces renseignements pour vous aider à vérifier le comportement de vos règles de filtrage d'URL basées sur la catégorie et la réputation.

Si vous êtes en désaccord avec la catégorisation, vous pouvez cliquer sur **Submit a URL Category Dispute** (Soumettre une contestation de catégorie d'URL) dans le FDM pour nous faire savoir ce que vous pensez.

Filtrage manuel des URL

Vous pouvez compléter ou remplacer de manière sélective le filtrage d'URL basé sur la catégorie et la réputation en filtrant manuellement des URL individuelles ou des groupes d'URL. Vous pouvez effectuer ce type de filtrage d'URL sans licence spéciale.

Par exemple, vous pourriez utiliser le contrôle d'accès pour bloquer une catégorie de sites Web qui ne conviennent pas à votre organisation. Toutefois, si la catégorie contient un site Web approprié et auquel vous souhaitez fournir l'accès, vous pouvez créer une règle Allow (Autoriser) manuelle pour ce site et la placer avant la règle Block (Bloquer) de la catégorie concernée.

Pour configurer le filtrage d'URL manuel, vous créez un objet URL avec l'URL de destination. La façon dont cette URL est interprétée dépend des règles suivantes :

- Si vous n'incluez pas de chemin (c'est-à-dire qu'il n'y a pas de caractères / dans l'URL), la correspondance est basée sur le nom d'hôte du serveur uniquement. Si vous incluez un ou plusieurs caractères /, la chaîne URL complète est utilisée pour une correspondance de sous-chaîne. Ainsi, une URL est considérée comme en correspondance si l'une des conditions suivantes est remplie :
  - La chaîne se trouve au début de l'URL.
  - La chaîne suit un point.
  - La chaîne contient un point au début.
  - La chaîne suit les caractères ://.

  Par exemple, ign.com correspond à ign.com ou www.ign.com, mais pas à versign.com.

Remarque Nous vous recommandons de ne pas utiliser le filtrage manuel d'URL pour bloquer ou autoriser des pages Web individuelles ou des parties de sites (c'est-à-dire les chaînes URL avec des caractères /), car les serveurs peuvent être réorganisés et les pages déplacées vers de nouveaux chemins.

- Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS). En d'autres termes, si vous bloquez un site Web, les trafics HTTP et HTTPS vers ce site Web sont bloqués, sauf si vous utilisez une condition d'application pour cibler un protocole spécifique. Lors de la création d'un objet URL, vous n'avez pas besoin de préciser le protocole lors de la création d'un objet. Par exemple, utilisez exemple.com plutôt que http://exemple.com.

- Si vous prévoyez utiliser un objet URL pour faire correspondre le trafic HTTPS dans une règle de contrôle d'accès, créez l'objet en utilisant le nom usuel du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic. De plus, le système ne tient pas compte des sous-domaines du nom usuel du sujet. N'incluez donc pas les informations de ce sous-domaine. Par exemple, utilisez exemple.com plutôt que www.exemple.com.

  Cependant, veuillez comprendre que le nom usuel du sujet dans le certificat peut être complètement sans rapport avec le nom de domaine d'un site Web. Par exemple, le nom usuel du sujet dans le certificat pour youtube.com est *.Google.com (bien entendu, cela peut changer à tout moment). Vous obtiendrez des résultats plus cohérents si vous utilisez la politique de déchiffrement SSL pour déchiffrer le trafic HTTPS afin que les règles de filtrage d'URL fonctionnent sur le trafic déchiffré.

Remarque Les objets URL ne correspondront pas au trafic HTTPS si le navigateur reprend une session TLS, car les informations de certificat ne sont plus disponibles. Ainsi, même si vous configurez soigneusement l'objet URL, vous pourriez obtenir des résultats incohérents pour les connexions HTTPS.

Filtrage du trafic HTTPS

Comme le trafic HTTPS est chiffré, effectuer le filtrage d'URL directement sur le trafic HTTPS n'est pas aussi simple que de le faire sur le trafic HTTP. Pour cette raison, vous devez envisager d'utiliser des politiques de déchiffrement SSL pour déchiffrer tout le trafic HTTPS que vous avez l'intention de filtrer. De cette façon, les politiques de contrôle d'accès de filtrage d'URL fonctionnent sur le trafic déchiffré, et vous obtenez les mêmes résultats que vous obtiendriez pour le trafic HTTP normal.

Toutefois, si vous avez l'intention d'autoriser qu'une partie du trafic HTTPS passe non déchiffré dans la politique de contrôle d'accès, vous devez comprendre que les règles font correspondre le trafic HTTPS différemment de ce qu'elles font pour le trafic HTTP. Pour filtrer le trafic chiffré, le système détermine l'URL demandée en fonction des informations transmises lors de la prise de contact SSL : le nom commun du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic. Il peut y avoir peu ou pas de relation entre le nom d'hôte du site Web dans l'URL et le nom commun du sujet.

Vous pouvez améliorer la mise en correspondance HTTPS pour les règles de catégorie/réputation si vous activez le filtrage des demandes DNS. Le système peut déterminer la catégorie et la réputation pendant la phase de résolution DNS et bloquer la réponse DNS pour les combinaisons indésirables, avant que l'utilisateur ne puisse commencer la tentative de connexion HTTPS. Pour les réponses DNS autorisées, le système disposera des informations de catégorie/réputation disponibles pour les connexions HTTPS ultérieures. Consultez Filtrage des requêtes DNS, à la page 12.

Le filtrage HTTPS, contrairement au filtrage HTTP, ne prend pas en compte les sous-domaines du nom commun du sujet. N'incluez pas d'informations de sous-domaine lors du filtrage manuel des URL HTTPS. Par exemple, utilisez exemple.com plutôt que www.exemple.com. Passez également en revue le contenu des certificats utilisés par le site pour vous assurer que vous avez le bon domaine, celui utilisé dans le nom commun du sujet, et que ce nom n'entrera pas en conflit avec vos autres règles (par exemple, le nom d'un site que vous souhaitez bloquer peut se chevaucher avec un que vous souhaitez autoriser). Par exemple, le nom usuel du sujet dans le certificat pour youtube.com est *.Google.com (bien entendu, cela peut changer à tout moment).

Remarque Les objets URL ne correspondront pas au trafic HTTPS si le navigateur reprend une session TLS, car les informations de certificat ne sont plus disponibles. Ainsi, même si vous configurez soigneusement l'objet URL, vous pourriez obtenir des résultats incohérents pour les connexions HTTPS.

Contrôle du trafic par le protocole de chiffrement

Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS) lors du filtrage d'URL. Cela se produit pour les conditions d'URL manuelles et basées sur la réputation. Autrement dit, le filtrage d'URL traite le trafic vers les sites Web suivants de manière identique :

- http://example.com
- https://example.com

Pour configurer une règle qui correspond uniquement au trafic HTTP ou HTTPS, mais pas aux deux, spécifiez soit le port TCP dans la condition de destination, soit ajoutez une condition d'application à la règle. Par exemple, vous pourriez autoriser l'accès HTTPS à un site tout en interdisant l'accès HTTP en créant deux règles de contrôle d'accès, chacune comportant une condition de port TCP, d'application et d'URL.

La première règle autorise le trafic HTTPS vers le site Web :

Action : Allow (Autoriser)
Port TCP ou application : HTTPS (port TCP 443)
URL : example.com

La deuxième règle bloque l'accès HTTP au même site Web :

Action : Bloc (Bloquer)
Port TCP ou application : HTTP (port TCP 80)
URL : example.com

Comparaison du filtrage d'URL et du filtrage d'applications

Les filtrages d'URL et d'application ont des similitudes. Vous devez toutefois les utiliser à des fins très distinctes :

- Le filtrage d'URL est mieux utilisé pour bloquer ou autoriser l'accès à l'ensemble d'un serveur Web. Par exemple, si vous ne souhaitez autoriser aucun type de jeux d'argent sur votre réseau, vous pouvez créer une règle de filtrage d'URL pour bloquer la catégorie Jeux. Avec cette règle, les utilisateurs ne peuvent accéder à aucune page sur aucun serveur Web dans la catégorie.
- Le filtrage des applications est utile pour bloquer des applications spécifiques, quel que soit le site d'hébergement, ou pour bloquer des fonctionnalités spécifiques d'un site Web par ailleurs autorisé. Par exemple, vous pourriez bloquer uniquement l'application Facebook Jeux sans bloquer tout Facebook.

Parce que la combinaison des critères d'application et d'URL peut entraîner des résultats inattendus, en particulier pour le trafic chiffré, il est bon de créer des règles distinctes pour les critères d'URL et d'application. Si vous devez combiner les critères d'application et d'URL dans une seule règle, vous devriez placer ces règles après les règles d'application uniquement ou d'URL uniquement, sauf si la règle application+URL agit comme une exception à une règle plus générale d'application uniquement ou d'URL uniquement. Étant donné que les règles de blocage de filtrage d'URL sont plus larges que le filtrage d'application, vous devez les placer au-dessus des règles d'application uniquement.

Si vous combinez les critères d'application et d'URL, vous devrez peut-être surveiller votre réseau de plus près pour vous assurer de ne pas autoriser l'accès aux sites et aux applications indésirables.

Bonnes pratiques pour un filtrage d'URL efficace

Veuillez garder les recommandations suivantes à l'esprit lorsque vous concevez vos règles de contrôle d'accès avec filtrage d'URL.

- Utilisez, chaque fois que possible, le blocage fondé sur la catégorie et la réputation. Cela garantit que les nouveaux sites sont automatiquement bloqués lorsqu'ils sont ajoutés aux catégories et que le blocage fondé sur la réputation est ajusté si un site devient plus (ou moins) fiable.
- Lorsque vous utilisez la mise en correspondance par catégorie d'URL, notez qu'il existe des cas où la page de connexion d'un site appartient à une catégorie différente de celle du site lui-même. Par exemple, Gmail se trouve dans la catégorie Web-based Email (Courriel Web), alors que la page de connexion se trouve dans la catégorie Search Engines and Portals (Moteurs de recherche et portails). Si vous avez des règles distinctes avec des actions différentes pour ces catégories, vous pourriez obtenir des résultats inattendus.
- Utilisez des objets d'URL pour cibler des sites Web entiers et créer des exceptions aux règles de blocage par catégorie. Autrement dit, pour autoriser des sites précis qui seraient autrement bloqués par une règle de catégorie.
- Si vous souhaitez bloquer manuellement un serveur Web (au moyen d'un objet d'URL), il est beaucoup plus efficace de le faire dans la politique Security Intelligence. La politique Security Intelligence rejette les connexions avant l'évaluation des règles de contrôle d'accès, ce qui permet un blocage plus rapide et plus efficace.
- Pour filtrer au mieux les connexions HTTPS, mettez en œuvre des règles de déchiffrement SSL pour déchiffrer le trafic auquel vous appliquez une règle de contrôle d'accès. Toute connexion HTTPS déchiffrée est traitée comme une connexion HTTP dans la politique de contrôle d'accès, ce qui vous permet d'éviter les limites propres au filtrage HTTPS.
- TLS 1.3 chiffre la plupart des messages d'établissement de liaison, de sorte que les renseignements sur les certificats ne sont pas facilement accessibles. Pour que le trafic chiffré avec TLS 1.3 corresponde efficacement aux règles d'accès qui utilisent le filtrage d'applications ou d'URL, le système doit obtenir un certificat en clair pour le serveur. Nous vous recommandons d'activer **TLS 1.3 Certificate Visibility (visibilité des certificats TLS 1.3)** dans les paramètres de contrôle d'accès. Si vous activez cette option, le système vérifie si un certificat pour le site est stocké en cache en fonction de l'adresse IP et de l'indication du nom du serveur (SNI) dans le paquet client « hello » Si aucun certificat n'est disponible, le système utilise une sonde TLS 1.2 pour obtenir le certificat, qui pourra ensuite être utilisé pour identifier la catégorie et la réputation de l'application ou de l'URL sans déchiffrer la connexion.
- Placez les règles de blocage d'URL avant toute règle de filtrage d'applications, car le filtrage d'URL bloque des serveurs Web entiers, alors que le filtrage d'applications cible une utilisation spécifique de l'application, quel que soit le serveur Web.
- Si vous souhaitez bloquer des sites à haut risque dont la catégorie est inconnue, sélectionnez la catégorie Uncategorized (Non classé) et ajustez le curseur de réputation sur Questionable (Douteux) ou Untrusted (Non fiable).
- Vous pouvez améliorer l'efficacité globale du filtrage d'URL en activant également le filtrage des demandes DNS. Lorsque vous utilisez le filtrage des demandes DNS, le système détermine la catégorie d'URL et la réputation du nom de domaine complet (FQDN) au moment de la recherche DNS, de sorte que l'information est disponible si une demande HTTP/HTTPS ultérieure vise la même destination. De

plus, si vous bloquez la catégorie ou la réputation, la tentative de connexion est arrêtée au stade de la demande DNS plutôt qu'au stade de l'établissement de la session Web. Consultez Filtrage des requêtes DNS, à la page 12.

Ce que l'utilisateur voit lorsque vous bloquez des sites Web

Lorsque vous bloquez des sites Web avec des règles de filtrage d'URL, ce que l'utilisateur voit diffère selon que le site est chiffré.

- Connexions HTTP : l'utilisateur voit une page de réponse de blocage par défaut du système au lieu de la page de navigateur normale pour les connexions expirées ou réinitialisées. Cette page doit indiquer clairement que la connexion a été bloquée intentionnellement.
- Connexions HTTPS (chiffrées) : l'utilisateur ne voit pas la page de réponse au blocage par défaut du système. Au lieu de cela, l'utilisateur voit la page par défaut du navigateur pour un échec de connexion sécurisée. 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. Ce message n'indique pas clairement que la connexion a été bloquée intentionnellement.

En outre, les sites Web peuvent être bloqués par d'autres règles de contrôle d'accès qui ne sont pas explicitement des règles de filtrage d'URL, ou même par l'action par défaut. Par exemple, si vous bloquez des réseaux entiers ou des géolocalisations, tous les sites Web de ce réseau ou de cet emplacement géographique sont également bloqués. Les utilisateurs bloqués par ces règles peuvent ou non obtenir une page de réponse comme décrit dans les limites ci-dessous.

Si vous mettez en œuvre le filtrage d'URL, pensez à expliquer aux utilisateurs finaux ce qu'ils peuvent voir lorsqu'un site est intentionnellement bloqué et les types de sites que vous bloquez. Sinon, ils pourraient passer beaucoup de temps à résoudre les connexions bloquées.

Limites des pages de réponse HTTP

Les pages de réponse HTTP ne s'affichent pas toujours lorsque le système bloque le trafic Web.

- Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué en raison d'une règle de contrôle d'accès promu (une règle de blocage placée tôt avec uniquement des conditions de réseau simples).
- Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué avant que le système ait identifié l'URL demandée.
- Le système n'affiche pas de page de réponse pour les connexions chiffrées bloquées par les règles de contrôle d'accès.

Filtrage des requêtes DNS

Vous pouvez appliquer la base de données de catégorie d'URL et de réputation aux demandes de recherche DNS, même pour les tentatives de connexion qui ne sont pas HTTP/HTTPS.

Par exemple, si un utilisateur tente d'établir une connexion FTP avec www.exemple.com, vous pouvez configurer le système pour rechercher la catégorie et la réputation de www.exemple.com lorsqu'il voit la demande de recherche DNS pour ce nom de domaine complet (FQDN). Si votre règle de filtrage DNS/URL pour la catégorie ou la réputation renvoyée est une règle de blocage, le système bloque la réponse DNS. Ainsi, l'utilisateur n'obtient pas d'adresse IP pour le FQDN et sa tentative de connexion échoue.

En activant le filtrage des demandes de recherche DNS, vous pouvez étendre vos règles de filtrage d'URL à des protocoles autres que HTTP/HTTPS, et empêcher les protocoles FTP, TFTP, SCP, ICMP et tout autre protocole d'établir une connexion avec un site que vous bloquez pour l'accès Web. Cela fonctionne tant que l'utilisateur utilise un nom FQDN et nécessite donc une recherche DNS. Si l'utilisateur utilise une adresse IP, il n'y a pas de demande DNS et le blocage des demandes DNS n'est pas possible.

Pour le trafic HTTP/HTTPS, la recherche de catégorie/réputation au moment de la demande DNS peut améliorer les performances du système, car cela peut empêcher la connexion avant la tentative d'établissement de la session Web. Cela peut être particulièrement utile pour HTTPS, qui est chiffré. En refusant au stade de la demande DNS, le système ne voit jamais de connexion HTTPS, et donc vos règles de déchiffrement n'ont pas besoin d'être évaluées, et le système n'a pas besoin d'effectuer la tâche plus difficile de faire correspondre une session chiffrée à la règle de contrôle d'accès appropriée.

Lignes directrices relatives au filtrage des demandes DNS

Gardez les éléments suivants à l'esprit lorsque vous configurez le filtrage de demande DNS :

- Le filtrage de demande DNS fonctionne uniquement sur la session DNS. Si vous autorisez la réponse DNS (c'est-à-dire si l'action de la règle de filtrage d'URL est Allow (Autoriser)), la connexion ultérieure que l'utilisateur établit avec l'adresse IP renvoyée sera évaluée séparément par rapport à vos règles de contrôle d'accès. La connexion peut correspondre à une règle différente et donc être bloquée ou autorisée pour d'autres raisons. Par exemple, si vous autorisez une tentative FTP d'obtenir une adresse IP par une recherche DNS, vous pouvez avoir une autre règle de contrôle d'accès qui interdise les connexions FTP, et la connexion sera finalement bloquée.
- Les demandes de recherche DNS qui correspondent aux règles de contrôle d'accès qui précèdent vos règles de filtrage de demande d'URL/DNS seront autorisées ou bloquées en fonction de la règle de correspondance. La recherche de catégorie/réputation ne sera pas effectuée pour ces connexions.
- Cette fonctionnalité nécessite que vous mettiez en œuvre le filtrage d'URL en fonction de la catégorie ou de la réputation. Vous devez avoir la licence de filtrage d'URL pour ce type de filtrage d'URL. Si vous n'avez aucune règle de filtrage d'URL en fonction de la catégorie/réputation, le filtrage de demande DNS n'est pas pertinent et vous ne devez pas l'activer.
- Les événements de connexion générés par le filtrage DNS incluent les champs suivants, particulièrement utiles : DNS Query (Requête DNS), URL Category (Catégorie d'URL) et URL Reputation (Réputation d'URL). Le champ DNS Query (Requête DNS) affiche le nom de domaine complet (FQDN) de la demande de recherche. Pour les événements de filtrage DNS, le champ URL sera vide.
- Le filtrage des requêtes DNS utilise uniquement la base de données de catégorie et de réputation d'URL. Tous les objets URL ou autres filtrages d'URL manuels définis dans une règle de contrôle d'accès correspondante sont ignorés. Si vous souhaitez mettre en œuvre le blocage de nom DNS manuel, utilisez la politique DNS Security Intelligence.

Filtrage des requêtes DNS en fonction de la catégorie d'URL et de la réputation

La procédure suivante explique comment mettre en œuvre le filtrage des demandes de recherche DNS.

Avant de commencer

Vous devez activer la licence d'URL si elle n'est pas déjà activée.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Access Control (Contrôle d'accès**.

Étape 2 Si nécessaire, cliquez sur le bouton **Access Policy Settings** (Paramètres de politique d'accès) ( ), sélectionnez l'option **Reputation Enforcement on DNS Traffic** (Application de la réputation sur le trafic DNS), puis cliquez sur **OK**.

Cette option active le filtrage des demandes DNS pour la politique de contrôle d'accès. Cette option est activée par défaut.

Étape 3 Évaluez les règles de filtrage d'URL existantes ou créez-en de nouvelles pour mettre en œuvre le filtrage en fonction de la catégorie d'URL et de la réputation qui s'appliquera également aux requêtes DNS.

Le filtrage d'URL s'applique normalement uniquement au trafic HTTP/HTTPS, il n'y a donc aucune raison de restreindre ces règles en fonction de l'application ou du port. Toutefois, si vous avez ces restrictions, assurez-vous que la règle peut également s'appliquer aux requêtes DNS :

- Dans l'onglet **Source/Destination**, si le champ **Destination Ports** (Ports de destination) comporte **Any** (N'importe quel), aucune modification n'est nécessaire. Si vous avez spécifié des ports, ajoutez **DNS sur UDP** et **DNS sur TCP** à la liste.
- Dans l'onglet **Applications**, si la liste des applications contient simplement **Any** (N'importe quel), aucune modification n'est nécessaire. Si vous avez spécifié des applications ou des filtres d'application, ajoutez l'application **DNS** à la liste ou au filtre. Les autres options liées au DNS ne sont pas pertinentes dans ce contexte.

Pour plus d'informations sur les règles de contrôle d'accès, consultez Configurer des règles de contrôle d'accès, à la page 21.

Étape 4 Évaluez les règles précédentes pour vous assurer que les requêtes DNS ne correspondent pas à ces règles.

La détermination de la catégorie et de la réputation se produit uniquement si la demande DNS correspond à une règle de filtrage d'URL qui comporte des spécifications de catégorie et de réputation. Toutes les demandes DNS qui correspondent à des règles antérieures dans la politique de contrôle d'accès à votre règle de filtrage d'URL contournent le filtrage de demande DNS. Ces requêtes DNS sont gérées selon la règle de correspondance, bloquées ou autorisées.

Inspection des intrusions, des fichiers et des logiciels malveillants

Les politiques de prévention des intrusions et de fichiers fonctionnent ensemble comme dernière ligne de défense avant que le trafic ne soit autorisé à atteindre sa destination :

- Les politiques de prévention des intrusions régissent les capacités de prévention des intrusions du système.
- Les politiques de fichiers régissent le contrôle des fichiers et les capacités de défense contre les programmes malveillants du système.

Tous les autres traitements de trafic ont lieu avant que le trafic réseau ne fasse l'objet d'un examen pour détecter les intrusions. En associant une politique de prévention des intrusions à une règle de contrôle d'accès,

vous informez le système qu'avant que ne soit transmis le trafic correspondant aux conditions de la règle de contrôle d'accès, vous souhaitez inspecter le trafic au moyen d'une politique de prévention des intrusions.

Vous pouvez configurer des politiques de prévention des intrusions et des fichiers uniquement sur des règles qui **autorisent** le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**). En outre, si l'action par défaut de la politique de contrôle d'accès est **allow**, vous pouvez configurer une politique de prévention des intrusions, mais pas une politique de fichiers.

Pour toute connexion unique gérée par une règle de contrôle d'accès, l'inspection des fichiers a lieu avant l'inspection de prévention des intrusions. C'est-à-dire que le système n'inspecte pas les fichiers bloqués par une politique de fichiers pour détecter les intrusions. Dans l'inspection des fichiers, le blocage simple par type prévaut sur l'inspection et le blocage des programmes malveillants. Jusqu'à ce qu'un fichier soit détecté et bloqué dans une session, les paquets de la session peuvent être soumis à une inspection de prévention des intrusions.

Remarque Par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers. L'inspection fonctionne uniquement avec le trafic non chiffré.

Bonnes pratiques pour l'ordre des règles de contrôle d'accès

Les règles sont appliquées sur la base de la première correspondance, vous devez donc vous assurer que les règles comprenant des critères de correspondance de trafic très spécifiques apparaissent au-dessus des politiques qui ont des critères plus généraux, qui s'appliqueraient autrement au trafic correspondant. Tenez compte des recommandations suivantes :

- Les règles spécifiques doivent précéder les règles générales, en particulier lorsqu'elles sont des exceptions aux règles générales.
- Toute règle qui rejette le trafic en se fondant uniquement sur des critères de couche 3/4 (comme l'adresse IP, la zone de sécurité et le numéro de port) devrait être placée le plus tôt possible. Nous vous recommandons de les placer avant toute règle nécessitant une inspection, comme celles avec des critères d'application ou d'URL, car les critères de la couche 3/4 peuvent être évalués rapidement et sans inspection. Bien entendu, toutes les exceptions à ces règles doivent être placées au-dessus.
- Chaque fois que cela est possible, mettez des règles de suppression spécifiques près du sommet de la politique. Cela garantit la prise de décision le plus tôt possible concernant le trafic indésirable.
- Les règles qui incluent à la fois des critères d'application et d'URL devraient être placées après les règles d'application uniquement ou d'URL uniquement, sauf si la règle application+URL constitue une exception à une règle plus générale d'application uniquement ou d'URL uniquement. Créez chaque fois que possible des règles distinctes pour le filtrage d'URL et d'application, car la combinaison des critères d'application et d'URL peut entraîner des résultats inattendus, en particulier pour le trafic chiffré.

NAT et critères d'accès

Les critères d'accès utilisent toujours les adresses IP réelles pour déterminer une correspondance, même si vous configurez la NAT. Par exemple, si vous configurez la NAT pour un serveur interne, 10.1.1.5, de sorte qu'il ait une adresse IP routable publiquement à l'extérieur, 209.165.201.5, alors le critère d'accès permettant

au trafic externe d'accéder au serveur interne doit faire référence à l'adresse IP réelle du serveur (10.1.1.5), et non à l'adresse mappée (209.165.201.5).

Comment les autres politiques de sécurité impactent le contrôle d'accès

D'autres politiques de sécurité peuvent affecter le fonctionnement des règles de contrôle d'accès et la mise en correspondance des connexions. Lors de la configuration de vos critères d'accès, gardez les éléments suivants à l'esprit :

- **SSL Decryption policy** (Politique de déchiffrement SSL) : les règles de déchiffrement SSL sont évaluées avant le contrôle d'accès. Ainsi, si une connexion chiffrée correspond à une règle de déchiffrement SSL appliquant un type de déchiffrement, c'est la connexion en clair (déchiffrée) qui est évaluée par la stratégie de contrôle d'accès. Les règles de contrôle d'accès ne voient pas la version chiffrée de la connexion. De plus, toute connexion correspondant à une règle de déchiffrement SSL qui abandonne le trafic n'est jamais vue par la stratégie de contrôle d'accès. Enfin, toute connexion chiffrée correspondant à une règle Do Not Decrypt (Ne pas déchiffrer) est évaluée dans son état chiffré.
- **Identity policy** (Politique d'identité) : les connexions sont mises en correspondance avec les utilisateurs (et donc les groupes d'utilisateurs) uniquement s'il existe un mappage utilisateur pour l'adresse IP source. Les critères d'accès fondées sur l'appartenance à un utilisateur ou à un groupe ne peuvent correspondre qu'aux connexions pour lesquelles l'identité de l'utilisateur a été collectée avec succès par votre politique d'identité.
- **Security Intelligence policy** (Politique de renseignements de sécurité) : toute connexion abandonnée n'est jamais vue par la stratégie de contrôle d'accès. Les connexions correspondant à la liste Do Not Block (Ne pas bloquer) sont ensuite comparées aux règles de contrôle d'accès et, en définitive, c'est la règle de contrôle d'accès qui détermine le traitement de la connexion (autorisée ou abandonnée).
- **VPN** (site à site ou accès à distance) : le trafic VPN est toujours évalué par rapport à la stratégie de contrôle d'accès, et les connexions sont autorisées ou abandonnées selon la règle correspondante. Toutefois, le tunnel VPN lui-même est déchiffré avant l'évaluation de la stratégie de contrôle d'accès. La stratégie de contrôle d'accès évalue les connexions encapsulées dans le tunnel VPN, et non le tunnel lui-même.

Exigences de licence pour le contrôle d'accès

Vous n'avez pas besoin d'une licence spéciale pour utiliser la politique de contrôle d'accès.

Cependant, vous avez besoin des licences suivantes pour des fonctionnalités spécifiques dans la politique de contrôle d'accès. Pour en savoir plus sur la configuration des licences, consultez Activation ou désactivation des licences facultatives.

- Licence **URL** : pour créer des règles qui utilisent les catégories d'URL et les réputations comme critères de correspondance.
- Licence **Menace** : pour configurer une politique de prévention des intrusions sur une règle d'accès ou l'action par défaut. Vous avez également besoin de cette licence pour utiliser une politique de fichiers (la licence Programme malveillant est également requise).
- Licence **Programme malveillant** : pour configurer une politique de fichiers sur une règle d'accès. Le Menace est également requis pour les politiques de fichiers.

Lignes directrices et limites pour les stratégies de contrôle d'accès

Voici quelques limites supplémentaires pour le contrôle d'accès. Veuillez en tenir compte lors de l'évaluation si vous obtenez les résultats attendus de vos règles.

- Si une mise à jour de la base de données d'URL comprend des catégories ajoutées (nouvelles, entrantes), obsolètes (sortantes) ou supprimées, il existe un délai de grâce pour vous permettre d'apporter des modifications aux règles de contrôle d'accès concernées. Les règles concernées sont marquées de messages d'information, avec des descriptions des problèmes qui ont une incidence sur la règle et des liens vers le site web Cisco Talos Intelligence Group (Talos) pour obtenir plus d'informations sur les changements de catégorie. Vous devez mettre à jour la règle afin qu'elle utilise les catégories appropriées disponibles dans la dernière base de données d'URL.

  Pour tenir compte du délai de grâce, ajoutez les catégories entrantes nouvellement ajoutées aux règles appropriées sans supprimer les catégories obsolètes sortantes : vos règles doivent contenir les nouvelles et les anciennes catégories. Les nouvelles catégories entreront en vigueur lorsque les anciennes catégories seront marquées pour suppression. Lorsque les anciennes catégories sont finalement supprimées, vous devez modifier les règles pour supprimer les catégories supprimées et redéployer la configuration. Vous ne pourrez pas déployer la configuration jusqu'à ce que vous corrigiez les règles utilisant les catégories supprimées. Cliquez sur le lien **See Problem Rules** (Voir les règles problématiques) au-dessus du tableau pour filtrer les règles qui nécessitent votre attention.

- FDM peut télécharger des informations sur un maximum de 50,000 utilisateurs à partir du serveur d'annuaire. Si votre serveur d'annuaire comprend plus de 50 000 comptes utilisateur, vous ne verrez pas tous les noms possibles lors de la sélection des utilisateurs dans une règle d'accès ou lors de l'affichage des informations de tableau de bord basé sur l'utilisateur. Vous pouvez écrire des règles uniquement sur les noms qui ont été téléchargés.

  La limite de 50 000 s'applique également aux noms associés aux groupes. Si un groupe compte plus de 50 000 membres, seuls les noms des 50 000 téléchargés peuvent être associés à l'appartenance au groupe.

- Si une mise à jour de la Vulnerability Database (VDB) retire (rend obsolètes) des applications, vous devez modifier toute règle de contrôle d'accès ou tout filtre d'application qui utilise l'application supprimée. Vous ne pouvez pas déployer les modifications avant d'avoir corrigé ces règles. En outre, vous ne pouvez pas installer les mises à jour du logiciel système avant de résoudre le problème. Dans la page d'objet des filtres d'application ou dans l'onglet Application de la règle, ces applications indiquent « (Deprecated) » (Obsolète) après le nom de l'application.

- Pour utiliser des objets réseau de nom de domaine complet (FQDN) comme critères de source ou de destination, vous devez également configurer DNS pour les interfaces de données dans **Device (Périphérique)** > **System Settings (Paramètres du système)** > **DNS Server (Serveur DNS)**. Le système n'utilise pas le paramètre du serveur DNS de gestion pour rechercher les objets de nom de domaine complet (FQDN) utilisés dans les règles de contrôle d'accès. Pour plus d'informations sur le dépannage de la résolution FQDN, consultez Dépannage des problèmes généraux de DNS.

  Notez que le contrôle de l'accès par nom de domaine complet (FQDN) est un mécanisme du meilleur effort. Prenez en compte les points suivants:

  - Étant donné que les réponses DNS peuvent être contrefaites, utilisez uniquement des serveurs DNS internes entièrement fiables.

  - Certains noms de domaine complets, en particulier pour les serveurs très populaires, peuvent avoir plusieurs adresses IP qui changent fréquemment. Comme le système utilise les résultats de recherche DNS en cache, les utilisateurs peuvent obtenir des adresses qui ne sont pas encore dans le cache. Ainsi, il est possible que le blocage d'un site populaire par FQDN produise des résultats incohérents.
  - Pour les noms de domaine complets populaires, différents serveurs DNS peuvent renvoyer un ensemble d'adresses IP différent. Ainsi, si vos utilisateurs utilisent un serveur DNS différent de celui que vous configurez, les règles de contrôle d'accès basé sur le nom de domaine complet (FQDN) pourraient ne pas s'appliquer à toutes les adresses IP du site qui sont utilisées par vos clients, et vous n'obtiendrez pas les résultats escomptés pour vos règles .
  - Certaines entrées de nom de domaine complet (FQDN) ont des valeurs de durée de vie très courte (TTL). Cela peut entraîner des recompilations fréquentes de la table de recherche, ce qui peut avoir une incidence sur les performances globales du système.

- Si vous modifiez une règle qui est activement utilisée, les modifications ne s'appliquent pas aux connexions établies qui ne sont plus inspectées par Snort. La nouvelle règle est utilisée pour la mise en correspondance avec les connexions futures. En outre, si Snort inspecte activement une connexion, il peut appliquer les critères de correspondance ou d'action modifiés à une connexion existante. Si vous devez vous assurer que vos modifications s'appliquent à toutes les connexions actuelles, vous pouvez vous connecter à l'interface de ligne de commande de l'appareil et utiliser la commande **clear conn** pour mettre fin aux connexions établies, en supposant que les sources tenteront ensuite de rétablir la connexion et seront ainsi correctement mises en correspondance avec la nouvelle règle.
- Il faut de 3 à 5 paquets pour que le système identifie l'application ou l'URL dans une connexion. Ainsi, la règle de contrôle d'accès correcte peut ne pas être mise en correspondance immédiatement pour une connexion donnée. Cependant, une fois que l'application ou l'URL est connue, la connexion est gérée en fonction de la règle de correspondance. Pour les connexions chiffrées, cela se produit après l'échange du certificat du serveur dans l'établissement de liaison SSL.
- Le système applique l'action de politique par défaut aux paquets qui n'ont pas de charge utile dans une connexion où une application est identifiée.
- 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. Par exemple, le système peut faire correspondre plus efficacement le trafic pour toutes les interfaces si vous laissez simplement les critères de zone de sécurité vides, plutôt que si vous créez des zones qui contiennent toutes les interfaces. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.
- Si vous spécifiez des adresses IP pour les critères de source ou de destination, ne combinez pas les adresses IPv4 et IPv6 dans la même règle. Créez des règles distinctes pour les adresses IPv4 et IPv6.
- Pendant son fonctionnement, le périphérique FTD étend les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu de tout objet de réseau utilisé dans la règle d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets réseau, mais recherche dans les critères d'accès les correspondances basées sur les définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos critères d'accès sont définies ou sur la façon dont elles s'affichent dans FDM. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès.

L'activation de la recherche de groupe d'objets réduit les besoins en mémoire pour les stratégies de contrôle d'accès qui incluent des objets réseau. Cependant, il est important de noter que la recherche par groupe d'objets peut également diminuer les performances de la recherche de règles et donc augmenter l'utilisation de l'unité centrale. Vous devez équilibrer l'incidence sur le processeur et le besoin en mémoire réduits pour la stratégie de contrôle d'accès spécifique. Dans la plupart des cas, l'activation de la recherche de groupe d'objets offre une nette amélioration opérationnelle.

Vous pouvez définir cette option à l'aide de FlexConfig en envoyant la commande **object-group-search access-control** ; utilisez la forme **no** de la commande dans le modèle de négation.

- Les tunnels GRE qui enfreignent les RFC associées seront rejetés. Par exemple, si un tunnel GRE contient des valeurs non nulles dans les bits réservés, contrairement aux RFC, il est rejeté. Si vous devez autoriser les tunnels GRE non conformes, vous devez utiliser un gestionnaire distant et configurer une règle de préfiltre qui fait confiance aux sessions. Vous ne pouvez pas configurer de règles de préfiltre à l'aide de FDM.

Configuration de la politique de contrôle d'accès

Utilisez la politique de contrôle d'accès pour contrôler l'accès aux ressources réseau. La politique consiste en un ensemble de règles ordonnées, qui sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic. Si aucune règle ne correspond au trafic, l'action par défaut affichée au bas de la page est appliquée.

Pour configurer la politique de contrôle d'accès, sélectionnez **Policies** > **Access Control**.

Le tableau de contrôle d'accès répertorie toutes les règles dans l'ordre. Pour chaque règle :

- Cliquez sur le bouton > à côté du numéro de la règle dans la colonne la plus à gauche pour ouvrir le diagramme de règles. Le diagramme peut vous aider à visualiser comment la règle contrôle le trafic. Cliquez sur le bouton de nouveau pour fermer le diagramme.
- La plupart des cellules permettent la modification en ligne. Par exemple, vous pouvez cliquer sur l'action pour en sélectionner une autre, ou cliquer sur un objet réseau source pour ajouter ou modifier les critères source.
- Pour déplacer une règle, passez la souris sur la règle jusqu'à ce qu'apparaisse l'icône de déplacement (), puis sélectionnez la règle (en cliquant dessus), faites-la glisser et déposez-la au nouvel emplacement. Vous pouvez également déplacer une règle en la modifiant et en sélectionnant le nouvel emplacement dans la liste de l'ordre (**Order**). Il est essentiel que vous définissiez les règles dans l'ordre dans lequel vous souhaitez qu'elles soient traitées. Des règles spécifiques doivent être près du sommet, en particulier pour les règles qui définissent des exceptions s'appliquant aux règles plus générales.
- La colonne la plus à droite contient les boutons d'action pour une règle; passez la souris sur la cellule pour voir les boutons. Vous pouvez modifier () ou supprimer () une règle.
- Cliquez sur le bouton des **paramètres de contrôle d'accès** () pour configurer les paramètres qui s'appliquent à la politique de contrôle d'accès, plutôt qu'à des règles spécifiques dans la politique.
- Cliquez sur l'icône **Toggle Hit Counts** () au-dessus du tableau pour ajouter ou supprimer la colonne du nombre d'accès (Hit Counts) dans le tableau. Cette colonne apparaît à droite de la colonne du nom. Elle présente le nombre total d'accès à la règle et la date et l'heure du dernier accès. Les informations

sur le nombre de visites sont extraites au moment où vous cliquez sur le bouton à bascule. Cliquez sur l'icône d'actualisation (**refresh**) ( ) pour obtenir les dernières informations.

- Si des règles rencontrent des problèmes, par exemple en raison de catégories d'URL supprimées ou modifiées, cliquez sur le lien **See Problem Rules** (voir les règles pour lesquelles il y a des problèmes) à côté de la zone de recherche pour filtrer le tableau afin d'afficher uniquement ces règles. Veuillez modifier et corriger (ou supprimer) ces règles afin qu'elles fournissent le service dont vous avez besoin.

Les rubriques suivantes expliquent comment configurer la politique.

Configuration de l'action par défaut

Si une connexion ne correspond pas à une règle d'accès spécifique, elle est gérée par l'action par défaut de la politique de contrôle d'accès.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez n'importe où dans le champ **Default Action** (action par défaut).

Étape 3 Sélectionnez l'action à appliquer au trafic correspondant.

- **Trust**(confiance) : autorisez le trafic sans autre inspection d'aucune sorte.
- **Allow** (autoriser) : autorisez le trafic soumis à la politique d'intrusion.
- **Block** (blocage) : abandonne le trafic sans condition. Le trafic n'est pas inspecté.

Étape 4 Si l'action est **Allow** (autoriser), sélectionnez une politique de prévention des intrusions.

Pour obtenir une explication des options, consultez Paramètres de la politique de prévention des intrusions, à la page 29.

Étape 5 (Facultatif) Configurez la journalisation pour l'action par défaut.

Vous devez activer la journalisation du trafic correspondant à la règle pour qu'elle soit incluse dans les données du tableau de bord ou le visualisateur d'événements. Consultez Paramètres de journalisation, à la page 31

Étape 6 Cliquez sur **OK**.

Configuration des paramètres de la politique de contrôle d'accès

Vous pouvez configurer des paramètres qui s'appliquent à la politique de contrôle d'accès plutôt qu'à des règles spécifiques au sein de cette politique.

Procédure

Étape 1 Sélectionnez **Policy (Politique)** > **Access Control (Contrôle d'accès)**.

Étape 2 Cliquez sur le bouton **Access Policy Settings** (Paramètres de la politique d'accès) ( ).

Étape 3 Configurez les paramètres.

- **TLS Server Identity Discovery** (Découverte de l'identité du serveur TLS) : TLS 1.3 chiffre la plupart des messages d'établissement de liaison, de sorte que les renseignements sur les certificats ne sont pas facilement accessibles. Pour que le trafic chiffré avec TLS 1.3 corresponde aux règles d'accès qui utilisent le filtrage d'applications ou d'URL, le système doit disposer d'un certificat en clair pour le serveur. Si vous activez cette option, le système vérifie si un certificat pour le site est stocké en cache en fonction de l'adresse IP et de l'indication du nom du serveur (SNI) dans le paquet client « hello ». Si aucun certificat n'est disponible, le système utilise une sonde TLS 1.2 pour obtenir le certificat, qui pourra ensuite être utilisé pour identifier la catégorie et la réputation de l'application ou de l'URL. Nous vous recommandons d'activer cette option pour vous assurer que les connexions chiffrées correspondent à la bonne règle de contrôle d'accès. Ce paramètre sert uniquement à obtenir le certificat ; la connexion reste chiffrée. L'activation de cette option suffit pour obtenir les certificats TLS 1.3 ; vous n'avez pas besoin de créer une règle de déchiffrement SSL correspondante. Cependant, les certificats mis en cache sont aussi utilisés pour optimiser le traitement des règles de déchiffrement, en plus du traitement de contrôle d'accès.
- **Reputation Enforcement on DNS Traffic** (Application de la réputation sur le trafic DNS) : activez cette option pour appliquer vos règles de catégorie et de réputation de filtrage d'URL aux demandes de résolution DNS. Si le nom de domaine complet (FQDN) dans la demande de recherche dispose d'une catégorie et d'une réputation que vous bloquez, le système bloque la réponse DNS. Étant donné que l'utilisateur ne reçoit pas de résolution DNS, l'utilisateur ne peut pas établir la connexion. Utilisez cette option pour appliquer un filtrage de catégorie et de réputation d'URL au trafic non Web. Pour en savoir plus, consultez Filtrage des requêtes DNS, à la page 12.

Étape 4 Cliquez sur **OK**.

Configurer des règles de contrôle d'accès

Utilisez les règles de contrôle d'accès pour contrôler l'accès aux ressources réseau. Les règles de la stratégie de contrôle d'accès sont évaluées de haut en bas. La règle appliquée au trafic est la première s'appliquant, entraînant la mise en correspondance de tous les critères de trafic.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Effectuez l'une des actions suivantes :

- Pour créer une nouvelle règle, cliquez sur le bouton **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle.

Pour supprimer une règle dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la règle.

Étape 3 Sous **Order**, sélectionnez l'endroit où vous souhaitez insérer la règle dans la liste ordonnée des règles.

Les règles sont appliquées sur la base de la première correspondance, vous devez donc vous assurer que les règles comprenant des critères de correspondance de trafic très spécifiques apparaissent au-dessus des politiques qui ont des critères plus généraux, qui s'appliqueraient autrement au trafic correspondant.

La valeur par défaut consiste à ajouter la règle à la fin de la liste. Si vous souhaitez modifier l'emplacement d'une règle ultérieurement, modifiez cette option.

Étape 4 Dans **Title** (titre), entrez un nom pour la règle.

Le nom ne peut pas contenir d'espaces. Vous pouvez utiliser des caractères alphanumériques et les caractères spéciaux suivants : +. _ -

Étape 5 Sélectionnez l'action à appliquer au trafic correspondant.

- **Trust**(confiance) : autorisez le trafic sans autre inspection d'aucune sorte.
- **Allow**(autorisation) : autorisez le trafic soumis à l'intrusion et à d'autres paramètres d'inspection dans la politique.
- **Block** (blocage) : abandonne le trafic sans condition. Le trafic n'est pas inspecté.

Étape 6 Définissez les critères de correspondance du trafic en utilisant n'importe quelle combinaison des onglets suivants :

- **Source/Destination** : zones de sécurité (interfaces) par lesquelles passe le trafic, adresses IP ou pays/continent (emplacement géographique) associé à l'adresse IP, balises de groupe de sécurité (SGT) attribuées à l'adresse, ou protocoles et ports utilisés par le trafic. La valeur par défaut englobe toute zone, adresse, emplacement géographique, SGT, protocole et port. Consultez Critères de source/de destination, à la page 23.
- **Application** : l'application ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est n'importe quelle application. Consultez Critères d'application, à la page 25.
- **URL** : URL ou catégorie d'URL d'une demande Web ou d'une recherche DNS. La valeur par défaut est toute URL. Consultez Critères pour les URL, à la page 27.
- **Users** (Utilisateurs) : la source d'identité, l'utilisateur ou le groupe d'utilisateurs. Vos politiques d'identité déterminent si les informations d'utilisateur et de groupe sont disponibles pour la correspondance du trafic. Vous devez configurer les politiques d'identité pour utiliser ce critère. Consultez Critères utilisateur, à la page 28.

Pour modifier une condition, vous cliquez sur le bouton + dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Si le critère requiert un objet, vous pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Lorsque vous ajoutez des conditions aux règles de contrôle d'accès, tenez compte des conseils suivants :

- Vous pouvez configurer plusieurs conditions par règle. Le trafic doit correspondre à toutes les conditions de la règle pour que celle-ci s'applique au trafic. Par exemple, vous pouvez utiliser une règle unique pour effectuer le filtrage d'URL pour des hôtes ou des réseaux spécifiques.
- Pour chaque condition d'une règle, vous pouvez ajouter jusqu'à 50 critères. Le trafic qui correspond à l'un des critères d'une condition satisfait à la condition. Par exemple, vous pouvez utiliser une règle unique pour appliquer le contrôle d'application à 50 applications ou filtres d'application. Ainsi, il existe une relation OU entre les éléments d'une condition unique, mais une relation ET entre les types de condition (par exemple, entre la source ou destination et l'application).
- Certaines fonctionnalités nécessitent l'activation de la licence appropriée.

Étape 7 (Facultatif) Pour les politiques qui utilisent l'action Allow (Autoriser), vous pouvez configurer une inspection plus approfondie du trafic non chiffré. Cliquez sur l'un des liens suivants :

- **Intrusion Policy** (Politique de prévention des intrusions) : sélectionnez **Intrusion Policy (Politique de prévention des intrusions)** > **On (Activer)**, puis sélectionnez la politique d'inspection des intrusions afin d'inspecter le trafic à la recherche d'intrusions et d'exploits. Consultez Paramètres de la politique de prévention des intrusions, à la page 29.
- **File Policy** (Politique de fichiers) : sélectionnez la politique de fichiers afin d'inspecter le trafic pour détecter les fichiers contenant des programmes malveillants et les fichiers à bloquer. Consultez Paramètres de la stratégie de fichier, à la page 30.

Étape 8 (Facultatif) Configurez la journalisation pour la règle.

Par défaut, les événements de connexion ne sont pas générés pour le trafic qui correspond à une règle, bien que les événements de fichier soient générés par défaut si vous sélectionnez une politique de fichiers. Vous pouvez modifier ce comportement. Vous devez activer la journalisation du trafic correspondant à la politique pour qu'il apparaisse dans les données des tableaux de bord ou dans Event Viewer (Visionneuse d'événements). Consultez Paramètres de journalisation, à la page 31.

Des incidents d'intrusion sont toujours générés pour toute règle de prévention des intrusions définie pour bloquer ou alerter, quelle que soit la configuration de journalisation de la règle de contrôle d'accès correspondante.

Étape 9 Cliquez sur **OK**.

Critères de source/de destination

Les critères Source/Destination d'une règle d'accès définissent les zones de sécurité (interfaces) par lesquelles passe le trafic, les adresses IP ou le pays ou le continent (emplacement géographique) pour l'adresse IP, les balises du groupe de sécurité (SGT) assignées à l'adresse, ou les protocoles et les ports utilisés dans le trafic. La valeur par défaut englobe toute zone, adresse, emplacement géographique, SGT, protocole et port.

Pour modifier une condition, vous cliquez sur le bouton **+** dans cette condition, sélectionnez l'objet ou l'élément souhaité, puis cliquez sur **OK**. Si le critère requiert un objet, vous pouvez cliquer sur **Create New *Object*** (créer un nouvel objet) si l'objet requis n'existe pas. Cliquez sur le **x** d'un objet ou d'un élément pour le supprimer de la politique.

Vous pouvez utiliser les critères suivants pour identifier la source et la destination à mettre en correspondance dans la règle.

Zones source, zones de destination

Les objets de la zone de sécurité qui définissent les interfaces par lesquelles passe le trafic. Vous pouvez définir un critère, les deux critères ou aucun critère : tout critère non spécifié s'applique au trafic sur n'importe quelle interface.

- Pour faire correspondre le trafic sortant de l'appareil depuis une interface dans la zone, ajoutez cette zone aux **zones de destination**.
- Pour faire correspondre le trafic entrant dans l'appareil depuis une interface dans la zone, ajoutez cette zone aux zones source (**Source Zones**).
- Si vous ajoutez des conditions de zone source et de zone de destination à une règle, le trafic correspondant doit provenir de l'une des zones source spécifiées et sortir par l'une des zones de destination.

Utilisez ces critères lorsque la règle doit être appliquée en fonction de l'entrée ou de la sortie du trafic sur l'appareil. Par exemple, si vous voulez vous assurer que tout le trafic destiné aux hôtes internes est

soumis à l'inspection d'intrusion, vous devez sélectionner votre zone interne comme **Destination Zones** (zones de destination) tout en laissant la zone source vide. Pour mettre en œuvre le filtrage des intrusions dans la règle, l'action liée à la règle doit être **Allow**(Autoriser), et vous devez sélectionner une politique de prévention des intrusions dans la règle.

Remarque Vous ne pouvez pas combiner des zones de sécurité passives et routées dans une seule règle. En outre, vous pouvez spécifier des zones de sécurité passives comme zones source uniquement, vous ne pouvez pas les spécifier comme zones de destination.

Réseaux sources, réseaux de destination

Les objets réseau ou les emplacements géographiques qui définissent les adresses réseau ou les emplacements du trafic.

- Pour faire correspondre le trafic d'une adresse IP ou d'un emplacement géographique, configurez les réseaux sources (**Source Networks**).
- Pour faire correspondre le trafic à une adresse IP ou à un emplacement géographique, configurez les réseaux de destination (**Source Networks**).
- Si vous ajoutez des conditions de réseau source et de destination à une règle, le trafic correspondant doit provenir de l'une des adresses IP spécifiées et être destiné à l'une des adresses IP de destination.

Lorsque vous ajoutez ce critère, vous sélectionnez les onglets suivants :

- **Network** (réseau) : Sélectionnez les objets ou groupes réseau qui définissent les adresses IP source ou de destination du trafic que vous souhaitez contrôler. Vous pouvez utiliser des objets qui définissent l'adresse utilisant le nom de domaine complet (FQDN); l'adresse est déterminée au moyen d'une recherche DNS.
- **Geolocation** (géolocalisation) : Sélectionnez l'emplacement géographique pour contrôler le trafic en fonction de son pays ou continent de source ou de destination. La sélection d'un continent sélectionne tous les pays du continent. En plus de sélectionner l'emplacement géographique directement dans la règle, vous pouvez également sélectionner un objet de géolocalisation que vous avez créé pour définir l'emplacement. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

Remarque Pour vous assurer que vous utilisez des données de localisation géographique à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Ports source, ports/protocoles de destination

Les objets de port qui définissent les protocoles utilisés dans le trafic. Pour TCP/UDP, cela peut inclure les ports. Pour ICMP, cela peut inclure des codes et des type.

- Pour faire correspondre le trafic d'un protocole ou d'un port, configurez les ports source (**Source Ports**). Les ports source peuvent uniquement être TCP/UDP.

- Pour faire correspondre le trafic à un protocole ou à un port, configurez les protocoles/ports de destination (**Destination Ports/Protocols**). Si vous n'ajoutez que des ports de destination à une condition, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Les spécifications ICMP et les autres spécifications non TCP/UDP sont autorisées dans les ports de destination uniquement; elles ne sont pas autorisées pour les ports source.
- Pour faire correspondre le trafic provenant de ports TCP/UDP spécifiques et destiné à des ports TCP/UDP spécifiques, configurez les deux. 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, vous pouvez cibler le trafic du port TCP/80 au port TCP/8080.

Groupes SGT source, groupes SGT de destination

Les objets de groupe de balise de groupe de sécurité (SGT) qui identifient les balises SGT affectées au trafic, tels qu'ils sont téléchargés à partir d'Identity Services Engine (ISE). Vous ne pouvez utiliser ces objets que si vous définissez une source d'identité Identity Services Engine (ISE) ; sinon, cette section ne s'affichera pas. Pour en savoir plus sur l'utilisation des balises SGT pour le contrôle d'accès, consultez Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec, à la page 35.

- Pour faire correspondre le trafic dont la source est l'une des balises SGT définies dans le groupe, configurez les **groupes SGT source**.
- Pour faire correspondre le trafic vers une destination dont l'une des balises SGT est définie dans le groupe, configurez les **groupes SGT de destination**.
- Si vous ajoutez des conditions de balise source et de destination à une règle, le trafic correspondant doit provenir d'une source avec l'une des balises spécifiées et être destiné à l'une des balises de destination.

Critères d'application

Les critères d'application d'une règle d'accès définissent l'application utilisée dans une connexion IP ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. La valeur par défaut est n'importe quelle application.

Bien que vous puissiez spécifier des applications individuelles dans la règle, les filtres d'applications simplifient la création et l'administration des politiques. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

De plus, Cisco met fréquemment à jour et ajoute des détecteurs d'applications supplémentaires par l'intermédiaire des mises à jour du système et de la base de données de vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Vous pouvez spécifier des applications et des filtres directement dans la règle, ou créer des objets de filtre d'application qui définissent ces caractéristiques. Les spécifications sont équivalentes, bien que l'utilisation d'objets puisse permettre de respecter plus facilement la limite du système de 50 éléments par critère si vous créez une règle complexe.

Pour modifier la liste des applications et des filtres, vous cliquez sur le bouton **+** dans la condition, sélectionnez les applications ou les objets de filtre d'application souhaités, qui sont répertoriés sur des onglets distincts, puis cliquez sur **OK** dans la boîte de dialogue contextuelle. Dans l'un ou l'autre des onglets, vous pouvez cliquer sur **Advanced Filter** (Filtres avancés) pour sélectionner des critères de filtre ou pour vous aider à rechercher des applications spécifiques. Cliquez sur le **x** pour une application, un filtre ou un objet pour le

supprimer de la politique. Cliquez sur le lien **Save As Filter** (Enregistrer en tant que filtre) pour enregistrer les critères combinés qui ne sont pas déjà un objet en tant que nouvel objet de filtre d'application.

Remarque Si une application sélectionnée a été supprimée par une mise à jour de VDB, « (Deprecated) » s'affiche après le nom de l'application. Vous devez supprimer ces applications du filtre, sinon les déploiements et les mises à niveau logicielles du système suivants seront bloqués.

Vous pouvez utiliser les critères **Advanced Filter** (Filtres avancés) suivants pour identifier l'application ou le filtre à mettre en correspondance dans la règle. Il s'agit des mêmes éléments utilisés dans les objets de filtre d'application.

Remarque Plusieurs sélections dans un seul critère de filtre ont une relation OU. Par exemple, le risque est élevé ou très élevé. La relation entre les filtres est ET, donc le risque est élevé ou très élevé, ET la pertinence commerciale est faible ou très faible. Lorsque vous sélectionnez des filtres, la liste des applications dans l'affichage est mise à jour pour n'afficher que celles qui répondent aux critères. Vous pouvez utiliser ces filtres pour vous aider à trouver les applications que vous souhaitez ajouter individuellement ou pour vérifier que vous sélectionnez les filtres souhaités à ajouter à la règle.

Risques

La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation, de très faible à très élevée.

Pertinence commerciale

La probabilité que l'application soit utilisée dans le cadre des activités professionnelles de votre entreprise, plutôt qu'à des fins récréatives, de très faible à très élevée.

Types

Le type d'application :

- **Application Protocol** (Protocole d'application) : protocoles d'application tels que HTTP et SSH, qui représentent les communications entre les hôtes.
- **Client Protocol** (Protocole client) : clients tels que les navigateurs Web et les clients de messagerie, qui représentent les logiciels s'exécutant sur l'hôte.
- **Web Application** (Application Web) : applications Web telles que MPEG video et Facebook, qui représentent le contenu ou l'URL demandée pour le trafic HTTP.

Catégories

Une classification générale de l'application qui décrit sa fonction la plus essentielle.

Étiquettes

Des informations supplémentaires sur l'application, similaires à la catégorie.

Pour le trafic chiffré, le système peut identifier et filtrer le trafic en utilisant uniquement les applications marquées **SSL Protocol** (Protocole SSL). Les applications sans cette balise ne peuvent être détectées que dans le trafic non chiffré ou déchiffré. Le système attribue la balise de **trafic déchiffré** aux applications qu'il peut détecter dans le trafic déchiffré uniquement, non chiffré ou non déchiffré.

Liste des applications (bas de l'affichage)

Cette liste est mise à jour à mesure que vous sélectionnez des filtres dans les options au-dessus de la liste, de sorte que vous pouvez voir les applications qui correspondent actuellement au filtre. Utilisez cette liste pour vérifier que votre filtre cible les applications souhaitées lorsque vous avez l'intention d'ajouter des critères de filtre à la règle. Si votre intention est d'ajouter des applications spécifiques, sélectionnez-les dans cette liste.

Critères pour les URL

Les critères d'URL d'une règle d'accès définissent l'URL utilisée dans une demande Web ou la catégorie à laquelle l'URL demandée appartient. Pour les correspondances de catégorie, vous pouvez également spécifier la réputation relative des sites à autoriser ou à bloquer. La valeur par défaut est d'autoriser toutes les URL.

Si vous activez le filtrage de la demande de recherche DNS, les paramètres de catégorie et de réputation s'appliquent également au nom de domaine complet (FQDN) dans la demande de recherche. Seuls les paramètres de catégorie et de réputation s'appliquent au filtrage de demande DNS. Le filtrage manuel des URL est ignoré.

Les catégories d'URL et les réputations vous permettent de créer rapidement des conditions d'URL pour les règles de contrôle d'accès. Par exemple, vous pourriez bloquer tous les sites de jeu ou les sites de non fiables. Si un utilisateur tente de rechercher une URL avec cette catégorie et cette combinaison de réputation, la session est bloquée.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Cela assure que le système contrôlera le trafic Web comme prévu. Enfin, comme les renseignements sur les menaces de Cisco sont continuellement mis à jour à la lumière de nouvelles URL, ainsi que de nouvelles catégories et risques pour les URL existantes, vous pouvez vous assurer que le système utilise des informations à jour pour filtrer les URL demandées. Les sites malveillants qui représentent des menaces de sécurité, comme les logiciels 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 de nouvelles politiques.

Pour modifier la liste d'URL, cliquez sur le bouton **+** dans la condition, puis sélectionnez les catégories ou les URL souhaitées à l'aide de l'une des techniques suivantes. Cliquez sur le **x** pour une catégorie ou un objet afin de le supprimer de la politique.

Onglet URL

Cliquez sur le signe **+**, sélectionnez des objets ou des groupes d'URL, puis cliquez sur **OK**. Vous pouvez cliquer sur **Create New URL** (Créer une nouvelle URL) si l'objet dont vous avez besoin n'existe pas.

Remarque Avant de configurer des objets URL pour cibler des sites spécifiques, lisez attentivement les informations sur le filtrage d'URL manuel.

Onglet Catégories

Cliquez sur **+**, sélectionnez les catégories souhaitées, puis cliquez sur **OK**.

Pour une description des catégories, consultez https://www.talosintelligence.com/categories.

La valeur par défaut est d'appliquer la règle à toutes les URL de chaque catégorie sélectionnée, quelle que soit leur réputation. Pour limiter la règle en fonction de la réputation, cliquez sur la flèche vers le bas pour chaque catégorie, désélectionnez la case **Any** (Tout), puis utilisez le curseur **Reputation** (Réputation) pour choisir le niveau de réputation. À la gauche du curseur de réputation, vous trouverez

de l'information sur les sites qui seront autorisés, tandis que les sites qui sont bloqués sont présentés du côté droit. La façon dont la réputation est utilisée dépend de l'action de la règle :

- Si la règle bloque ou surveille l'accès Web, la sélection d'un niveau de réputation sélectionne également toutes les réputations plus graves que ce niveau. Par exemple, si vous configurez une règle pour bloquer ou surveiller les sites (Suspects) et **Questionable** (Discutables) (niveau 2), elle bloque également automatiquement les sites (À risque élevé) et **Untrusted** (Non fiables) (niveau 1).
- Si la règle autorise l'accès Web, la sélection d'un niveau de réputation sélectionne également toutes les réputations moins graves que ce niveau. Par exemple, si vous configurez une règle pour autoriser les sites (Bénins) et **Favorable** (Favorables) (niveau 4), elle autorise également automatiquement les sites (Bien connus) et **Trusted (de confiance)** (niveau 5).

Sélectionnez l'option **Include Sites with Unknown Reputation** (inclure les sites avec une réputation inconnue) pour inclure les URL de réputation inconnue dans la correspondance de réputation. Les nouveaux sites ne sont généralement pas classés, et il peut y avoir d'autres raisons pour lesquelles la réputation d'un site est inconnue ou ne peut être déterminée.

Vérifier la catégorie d'une URL

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Saisissez l'URL dans le champ **URL to Check** (URL à vérifier), puis cliquez sur **Go** (Lancer). Vous serez redirigé vers un site Web externe pour consulter les résultats. Si vous êtes en désaccord avec une catégorisation, cliquez sur le lien **Submit a URL Category** Dispute (Soumettre une contestation de catégorie d'URL) et faites-le-nous savoir.

Critères utilisateur

Les critères utilisateur d'une règle d'accès définissent l'utilisateur ou le groupe d'utilisateurs pour une connexion IP. Vous devez configurer les politiques d'identité et le serveur d'annuaire associé pour inclure les critères d'utilisateur ou de groupe d'utilisateurs dans une règle d'accès.

Vos politiques d'identité déterminent si l'identité de l'utilisateur est collectée pour une connexion particulière. Si l'identité est établie, l'adresse IP de l'hôte est associée à l'utilisateur identifié. Ainsi, le trafic dont l'adresse IP source est mappée à un utilisateur est considéré comme provenant de cet utilisateur. Les paquets IP en eux-mêmes ne comprennent pas d'informations sur l'identité de l'utilisateur, de sorte que ce mappage adresse IP-utilisateur est la meilleure approximation disponible.

Étant donné que vous pouvez ajouter un maximum de 50 utilisateurs ou groupes à une règle, il est généralement plus logique de sélectionner des groupes que de sélectionner des utilisateurs individuels. Par exemple, vous pouvez créer une règle autorisant le groupe d'ingénierie à accéder à un réseau de développement, puis créer une règle ultérieure qui refuse tout autre accès au réseau. Ensuite, pour que la règle s'applique aux nouveaux ingénieurs, il vous suffit d'ajouter le spécialiste en ingénierie au groupe Engineering dans le serveur d'annuaire.

Vous pouvez également sélectionner les sources d'identité à appliquer à tous les utilisateurs de cette source. Ainsi, si vous prenez en charge plusieurs domaines Active Directory, vous pouvez fournir un accès différentiel aux ressources en fonction du domaine.

Pour modifier la liste des utilisateurs, vous cliquez sur le bouton **+** dans la condition et sélectionnez les identités souhaitées en utilisant l'une des techniques suivantes. Cliquez sur le **x** pour supprimer une identité de la politique.

- **Sources d'identité** : sélectionnez une source d'identité, telle qu'un domaine AD ou la base de données d'utilisateurs locaux, pour appliquer la règle à tous les utilisateurs obtenus à partir des sources

sélectionnées. Si le domaine dont vous avez besoin n'existe pas encore, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité) et créez-le maintenant.

- **Groupes** : sélectionnez les groupes d'utilisateurs souhaités. Les groupes sont disponibles uniquement si vous les configurez dans le serveur de répertoire. Si vous sélectionnez un groupe, la règle s'applique à tous les membres du groupe, y compris les sous-groupes. Si vous souhaitez traiter un sous-groupe différemment, vous devez créer une règle d'accès distincte pour le sous-groupe et la placer au-dessus de la règle pour le groupe parent dans la stratégie de contrôle d'accès.
- **Utilisateurs** : sélectionnez des utilisateurs individuels. Le nom d'utilisateur est précédé de la source d'identité, par exemple Realm\username (domaine\nom_utilisateur).

  Il existe certains utilisateurs intégrés dans le domaine Special-Identities-Realm (domaine d'identités spéciales) :

  - **Failed Authentication** (Échec de l'authentification) : l'utilisateur a été invité à s'authentifier, mais n'a pas réussi à saisir une paire nom d'utilisateur/mot de passe valide dans le nombre maximal de tentatives autorisées. L'échec de l'authentification n'empêche pas l'utilisateur d'accéder au réseau, mais vous pouvez écrire une règle d'accès pour limiter l'accès au réseau pour ces utilisateurs.
  - **Guest** (Invité) : les utilisateurs invités sont similaires aux utilisateurs en Failed Authentication (Échec de l'authentification), sauf que votre règle d'identité est configurée pour identifier ces utilisateurs comme Guest (Invité). Les utilisateurs invités ont été invités à s'authentifier et n'ont pas réussi à le faire dans les limites du nombre maximal de tentatives.
  - **No Authentication Required** (Aucune authentification requise) : l'utilisateur n'a pas été invité à s'authentifier, car ses connexions correspondaient à des règles d'identité ne spécifiant aucune authentification.
  - **Unknown** (Inconnu) : aucun mappage d'utilisateur n'existe pour l'adresse IP et aucun échec d'authentification n'a encore été enregistré. En règle générale, cela signifie qu'aucun trafic HTTP n'a encore été vu à partir de cette adresse.

Paramètres de la politique de prévention des intrusions

Cisco fournit plusieurs politiques d'intrusion avec le système de pare-feu. Les politiques d'intrusion fournies par Cisco Cisco Talos Intelligence Group (Talos) sont conçues par le Cisco.Talos, qui définit les états des règles d'intrusion et de préprocesseur ainsi que les paramètres avancés. Pour les règles de contrôle d'accès qui autorisent le trafic, vous pouvez sélectionner une politique d'intrusion pour inspecter le trafic à la recherche d'intrusions et d'exploits. Une politique de prévention des intrusions examine les paquets décodés à la recherche d'attaques basées sur des modèles, et peut bloquer ou modifier le trafic malveillant.

Lors de l'exécution de Snort 2, ce sont les seules politiques disponibles et vous ne pouvez pas les modifier. Cependant, vous pouvez modifier l'action à prendre pour une règle donnée, comme décrit dans Modification des actions des règles de prévention des intrusions (Snort 2).

Lors de l'exécution de Snort 3, vous pouvez sélectionner l'une de ces politiques ou créer vos propres politiques d'intrusion.

Pour activer l'inspection des intrusions, sélectionnez **Intrusion Policy (Politique d'intrusion)** > **On (Activée)** et sélectionnez la politique souhaitée. Cliquez sur l'icône d'information d'une politique dans la liste déroulante pour afficher une description pour chaque politique.

Pour en savoir plus sur les politiques prédéfinies, consultez Politiques d'analyse de réseau et de prévention des intrusions définies par le système.

Paramètres de la stratégie de fichier

Utilisez les politiques de fichiers pour détecter les programmes malveillants, ou *malware*, au moyen de la défense contre les logiciels malveillants. Vous pouvez également utiliser les politiques de fichiers pour effectuer le contrôle de fichier, ce qui permet de contrôler tous les fichiers d'un type spécifique, qu'ils contiennent ou non des logiciels malveillants.

La défense contre les logiciels malveillants utilise le Cisco AMP Cloud pour récupérer les dispositions relatives aux éventuels programmes malveillants détectés dans le trafic réseau, et pour obtenir des analyses locales de programmes malveillants et des mises à jour de pré-classification de fichiers. L'interface de gestion doit disposer d'un chemin vers Internet pour atteindre Cisco AMP Cloud et effectuer des recherches de programmes malveillants. Lorsque l'appareil détecte un fichier admissible, il utilise la valeur de hachage SHA-256 du fichier pour demander la Cisco AMP Cloud disposition du fichier. Les dispositions possibles sont les suivantes :

- Malware (Programmes malveillants) : le Cisco AMP Cloud a classé le fichier comme un logiciel malveillant. Un fichier d'archive (p. ex. un fichier compressé) est marqué comme malveillant si un de ses fichiers est malveillant.
- Clean (Propre : le Cisco AMP Cloud a classé le fichier comme propre, ne contenant aucun logiciel malveillant. Un fichier d'archive est marqué comme propre si tous les fichiers qu'il contient le sont.
- Unknown (Inconnu) : le Cisco AMP Cloud n'a pas encore affecté de disposition au fichier. Un fichier d'archive est marqué comme inconnu s'il contient un fichier inconnu.
- Unavailable (Non disponible) : le système n'a pas pu interroger le Cisco AMP Cloud pour déterminer la disposition du fichier. Vous pouvez voir un faible pourcentage d'événements avec cette disposition; c'est un comportement attendu. Si vous voyez un certain nombre d'événements « indisponible » se succéder, assurez-vous que la connexion Internet fonctionne correctement pour l'adresse de gestion.

Politiques de fichiers disponibles

Vous pouvez sélectionner l'une des politiques de fichiers suivantes :

- **Aucun** : n'évalue pas les fichiers transmis à la recherche de programmes malveillants et n'effectue aucun blocage spécifique aux fichiers. Sélectionnez cette option pour les règles dans lesquelles les transmissions de fichiers sont sécurisées ou lorsqu'elles sont peu probables (ou impossibles), ou pour les règles pour lesquelles vous êtes sûr que votre filtrage d'application ou d'URL protège adéquatement votre réseau.
- **Block Malware All** (Bloquer tous les programmes malveillants) : interrogez le Cisco AMP Cloudpour déterminer si des fichiers traversant votre réseau contiennent des programmes malveillants, puis bloquez les fichiers qui représentent des menaces.
- **Cloud Lookup All (Recherche dans le nuage pour tous)** : interrogez le Cisco AMP Cloud pour obtenir et consigner la disposition des fichiers traversant votre réseau, tout en autorisant leur transmission.
- **(Custom File Policy)** (Politique de fichiers personnalisée) : vous pouvez créer vos propres politiques de fichiers à l'aide de la ressource API filepolicies Cisco Firepower Threat Defense et des autres ressources FileAndMalwarePolicies (telles que filetypes, filetypecategories, ampcloudconfig, ampservers et ampcloudconnections). Après avoir créé les politiques et déployé les modifications, vous pouvez sélectionner vos politiques lors de la modification d'une règle de contrôle d'accès dans FDM. La description de la politique s'affiche sous la politique lorsque vous la sélectionnez.

Paramètres de journalisation

Les paramètres de journalisation d'une règle d'accès déterminent si les événements de connexion sont émis pour le trafic qui correspond à la règle. Vous devez activer la journalisation pour voir les événements liés à la règle dans la visionneuse d'événements. Vous devez également activer la journalisation pour que le trafic correspondant soit reflété dans les différents tableaux de bord que vous pouvez utiliser pour surveiller le système.

Vous devez enregistrer les connexions en fonction des besoins de sécurité et de conformité de votre entreprise. Si votre objectif est de limiter le nombre d'événements que vous générez et d'améliorer les rendements, activez la journalisation uniquement pour les connexions essentielles à votre analyse. Toutefois, si vous souhaitez obtenir une vue d'ensemble de votre trafic réseau à des fins de profilage, vous pouvez activer la journalisation pour des connexions supplémentaires.

Mise en garde La journalisation des connexions TCP bloquées lors d'une attaque par déni de service (DoS) peut affecter le rendement du système et submerger la base de données avec plusieurs événements similaires. Avant d'activer la journalisation pour une règle de blocage, déterminez si la règle concerne une interface Internet ou une autre interface vulnérable aux attaques DoS.

Vous pouvez configurer les actions de journalisation suivantes.

Sélectionner l'action de journalisation

Vous pouvez sélectionner l'une des actions suivantes :

- **Log at Beginning and End of Connection** (Journaliser au début et à la fin de la connexion) : émet des événements au début et à la fin d'une connexion. Comme les événements de fin de connexion contiennent tout ce que contiennent les événements de début de connexion, ainsi que toutes les informations qui peuvent être obtenues au cours de la connexion, Cisco vous recommande de ne pas sélectionner cette option pour le trafic que vous autorisez. La journalisation de ces deux événements peut avoir une incidence sur les performances du système. Cependant, il s'agit de la seule option autorisée pour le trafic bloqué.
- **Log at End of Connection** (Journaliser à la fin de la connexion) : sélectionnez cette option si vous souhaitez activer la journalisation des connexions à la fin de la connexion, ce qui est recommandé pour le trafic autorisé ou de confiance.
- **No Logging at Connection** (Aucune journalisation à la connexion) : sélectionnez cette option pour désactiver la journalisation pour la règle. Il s'agit du paramètre par défaut.

Remarque Lorsqu'une politique de prévention des intrusions, invoquée par une règle de contrôle d'accès, détecte une intrusion et génère un événement d'intrusion, le système consigne automatiquement la fin de la connexion où l'intrusion s'est produite, quelle que soit la configuration de journalisation de la règle. Pour les connexions où une intrusion a été bloquée, l'action pour la connexion dans le journal de connexion est **Bloc**k (blocage), avec un motif **Intrusion Block** (blocage d'intrusion), même si, pour effectuer une inspection de prévention des intrusions, vous devez utiliser une règle Allow (autoriser).

Événements liés aux fichiers

Sélectionnez **Log Files** (Journaliser les fichiers) si vous souhaitez activer la journalisation des fichiers interdits ou des événements de programmes malveillants. Vous devez sélectionner une politique de

fichiers dans la règle pour configurer cette option. L'option est activée par défaut si vous sélectionnez une politique de fichiers pour la règle. Cisco vous recommande de laisser cette option activée.

Lorsque le système détecte un fichier interdit, il consigne automatiquement l'un des types d'événement suivants :

- *File events* (événements de fichier), qui représentent les fichiers détectés ou bloqués, y compris les fichiers de programmes malveillants
- *Malware events* (événements de programmes malveillants), qui représentent uniquement les fichiers de programmes malveillants détectés ou bloqués
- *Retrospective malware events* (événements rétrospectifs de programme malveillant), qui sont générés lorsque la disposition de programme malveillant pour un fichier détecté précédemment change.

Pour les connexions où un fichier a été bloqué, l'action pour la connexion dans le journal de connexion est **Block** (blocage), même si, pour effectuer l'inspection des fichiers et des programmes malveillants, vous devez utiliser une règle Allow (autoriser). Le motif de la connexion (Reason) est soit **File Monitor** (surveillance de fichier, lorsqu'un type de fichier ou un programme malveillant a été détecté), soit **Malware Block** (blocage de programme malveillant) ou **File Block** (blocage de fichier), lorsqu'un fichier a été bloqué.

Envoyer les événements de connexion à :

Si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Create New Syslog Server** (Créer un nouveau serveur syslog) et créez-le. (Pour désactiver la journalisation sur un serveur syslog, sélectionnez **Any** (tout) dans la liste des serveurs.)

Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.

Ce paramètre s'applique uniquement aux événements de connexion. Pour envoyer les incidents d'intrusion à syslog, configurez le serveur dans les paramètres de la politique de prévention des intrusions. Pour envoyer des événements de fichier ou de programme malveillant à syslog, configurez le serveur dans **Device (Appareil)** > **System Settings (Paramètres du système)** > **Logging Settings (Paramètres de journalisation)**.

Gestion des stratégies de contrôle d'accès

Les rubriques suivantes expliquent comment vous pouvez surveiller la stratégie de contrôle d'accès.

Statistiques de contrôle d'accès dans les tableaux de bord

La plupart des données sur les tableaux de bord **Monitoring** (Surveillance) sont directement liées à votre politique de contrôle d'accès. Consultez Tableaux de bord du trafic et du système.

- **Monitoring (Surveillance)** > **Access And SI Rules (Règles d'accès et SI)** affiche les règles d'accès les plus sollicitées, les équivalents de règles Security Intelligence et les statistiques associées.
- Vous pouvez trouver des statistiques générales dans les tableaux de bord **Network Overview** (Aperçu du réseau), **Destinations** et **Zones**.

- Vous pouvez trouver les résultats du filtrage d'URL dans les tableaux de bord (Catégories Web)**URL Categories** (Catégories d'URL) et **Destinations**. Vous devez avoir au moins une politique de filtrage d'URL pour voir des informations sur le tableau de bord **URL Categories (Catégories d'URL).**.
- Vous pouvez trouver les résultats du filtrage des applications dans les tableaux de bord **Applications** et **Web Applications** (Applications Web).
- Vous pouvez trouver des statistiques basées sur les utilisateurs dans le tableau de bord **Users** (Utilisateurs). Vous devez mettre en œuvre des politiques d'identité pour recueillir les informations sur les utilisateurs.
- Vous pouvez trouver les statistiques relatives aux politiques de prévention des intrusions dans les tableaux de bord **Attackers** (Attaquants) et **Targets** (Cibles). Vous devez appliquer une politique de prévention des intrusions à au moins une règle de contrôle d'accès pour voir des informations dans ces tableaux de bord.
- Vous pouvez trouver les statistiques de politique de fichiers et de filtrage de programmes malveillants dans les tableaux de bord **File Logs** (Journaux de fichiers) et **Malware** (Programmes malveillants). Vous devez appliquer une politique de fichiers à au moins une règle de contrôle d'accès pour voir des informations dans ces tableaux de bord.
- **Monitoring (Surveillance)** > **Events (Événements)** affiche aussi les événements pour les connexions et les données liées aux règles de contrôle d'accès.

Examen du nombre de résultats pour les règles

Vous pouvez désormais afficher le nombre de résultats pour les règles de contrôle d'accès. Le nombre de résultats indique le nombre de connexions correspondant à la règle. Vous pouvez utiliser ces renseignements pour identifier les règles les plus actives et les règles qui sont moins actives.

Le nombre provient du dernier redémarrage du système, que ce soit à partir de votre action ou d'une mise à niveau du système, ou du moment où vous réinitialisez le nombre de résultats pour une règle ou toutes les règles.

Vous pouvez également afficher les informations sur le nombre de résultats dans les règles dans l'interface de ligne de commande du périphérique en utilisant la commande **show rule hits**.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez sur l'icône **Toggle Hit Counts** (Bascule du nombre de résultats) ( ).

Cette colonne apparaît à droite de la colonne du nom. Elle présente le nombre total d'accès à la règle et la date et l'heure du dernier accès. Les informations sur le nombre de visites sont extraites au moment où vous cliquez sur le bouton à bascule.

Vous pouvez effectuer les opérations suivantes avec les informations du nombre de résultats :

- À gauche du bouton, vous verrez des informations sur la dernière mise à jour du nombre de résultats.

  Cliquez sur l'icône **Refresh** (Actualiser) ( ) pour obtenir les derniers chiffres.
- Pour ouvrir une vue détaillée du nombre de résultats pour une règle donnée, cliquez sur le numéro de nombre de résultats dans le tableau pour ouvrir la boîte de dialogue Hit Count (Nombre de résultats).

Les informations sur le nombre de résultats comprennent le nombre de résultats ainsi que la date et l'heure de la dernière connexion qui correspond à la règle. Cliquez sur le lien **Reset** (Réinitialiser pour réinitialiser le compteur à zéro.

Si vous souhaitez réinitialiser le nombre de résultats pour toutes les règles en même temps, ouvrez une session SSH sur le périphérique et lancez la commande **clear rule hits**.

- Cliquez à nouveau sur l'icône **Toggle Hit Counts** (Bascule du nombre de résultats) ( ) pour supprimer la colonne du nombre d'accès (Hit Counts) du tableau.

Surveillance des messages Syslog pour le contrôle d'accès

En plus de voir les événements dans la visionneuse d'événements, vous pouvez configurer les règles de contrôle d'accès, les politiques de prévention des intrusions, les politiques de fichiers/programmes malveillants, et les politiques de Security Intelligence pour envoyer des événements à un serveur syslog. Les événements utilisent les ID de message suivants :

- 430001 : événement d'intrusion.
- 430002 : événement de connexion journalisé au début d'une connexion.
- 430003 : événement de connexion enregistré à la fin d'une connexion.
- 430004 : événements de fichier.
- 430005 : événements de programme malveillant.

Surveillance des stratégies de contrôle d'accès dans l'interface de ligne de commande

Vous pouvez également ouvrir la console d'interface de ligne de commande ou vous connecter à l'interface de ligne de commande du périphérique et utiliser les commandes suivantes pour obtenir des informations plus détaillées sur les stratégies de contrôle d'accès et les statistiques.

- **show access-control-config** affiche des informations récapitulatives sur les règles de contrôle d'accès ainsi que le nombre de résultats par règle.
- **show access-list** affiche les listes de contrôle d'accès (ACL) générées à partir des règles de contrôle d'accès. Les listes de contrôle d'accès fournissent un filtre initial et permettent de prendre rapidement des décisions lorsque c'est possible, afin que les connexions devant être abandonnées n'aient pas à être inspectées (et ne consomment donc pas de ressources inutilement). Ces renseignements comprennent le nombre de résultats.
- **show rule hits** affiche le nombre de résultats consolidés qui sont plus précis que les chiffres affichés avec **show access-control-config** et **show access-list**. Si vous souhaitez réinitialiser le nombre de résultats, utilisez la commande **clear rule hits**.
- **show snort statistics** affiche les renseignements sur le moteur d'inspection Snort, qui est l'inspecteur principal. Snort met en œuvre le filtrage des applications, le filtrage des URL, la protection contre les intrusions et le filtrage des fichiers et des programmes malveillants.

- **show conn** affiche des renseignements sur les connexions actuellement établies par l'intermédiaire des interfaces.
- **show traffic** affiche les statistiques sur le trafic circulant dans chaque interface.
- **show ipv6 traffic** affiche les statistiques sur le trafic IPv6 circulant dans le périphérique.

Exemples pour le contrôle d'accès

Le chapitre sur les cas d'utilisation comprend plusieurs exemples de mise en œuvre des règles de contrôle d'accès. Consultez les exemples suivants.

- Comment mieux comprendre le trafic de votre réseau. Cet exemple montre quelques concepts de base pour la collecte d'informations globales sur les connexions et les utilisateurs.
- Comment bloquer les menaces. Cet exemple montre comment appliquer les politiques de prévention des intrusions.
- Comment bloquer les logiciels malveillants. Cet exemple montre comment appliquer les politiques de fichiers.
- Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL). Cet exemple montre comment effectuer le filtrage d'URL.
- Comment contrôler l'utilisation des applications. Cet exemple montre comment effectuer le filtrage d'applications.
- Comment ajouter un sous-réseau. Cet exemple montre comment intégrer un nouveau sous-réseau à votre réseau global, y compris les règles d'accès nécessaires pour permettre la circulation du trafic.
- Comment surveiller passivement le trafic sur un réseau

Voici des exemples supplémentaires.

Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec

Si vous utilisez le moteur de services d'identité de Cisco (ISE) pour définir et utiliser la balise de groupe de sécurité (SGT) pour classer le trafic dans un réseau Cisco TrustSec, vous pouvez écrire des règles de contrôle d'accès qui utilisent la SGT comme critère de correspondance. Ainsi, vous pouvez bloquer ou autoriser l'accès en fonction de l'appartenance au groupe de sécurité plutôt que par rapport à des adresses IP.

À propos des balises de groupe de sécurité (SGT)

Dans Cisco Identity Services Engine (ISE), vous pouvez créer des balises de groupe de sécurité (SGT) et attribuer des adresses IP d'hôte ou de réseau à chaque balise. Vous pouvez également affecter des SGT aux comptes utilisateur, et la SGT est affectée au trafic de l'utilisateur. Si les commutateurs et les routeurs du réseau sont configurés pour le faire, ces balises sont ensuite affectées aux paquets à mesure qu'ils entrent dans le réseau contrôlé par ISE, le nuage Cisco TrustSec.

Lorsque vous configurez une source d'identité ISE dans le FDM, le système Cisco Firepower Threat Defense télécharge automatiquement la liste des SGT à partir d'ISE. Vous pouvez ensuite utiliser SGT comme condition de correspondance de trafic dans les règles de contrôle d'accès.

Par exemple, vous pourriez créer une balise Utilisateurs de production et associer le réseau 192.168.7.0/24 à la balise. Ce serait approprié si vous utilisez ce réseau pour les points d'extrémité des utilisateurs, tels que les ordinateurs portables, les clients Wi-Fi, etc. Vous pourriez créer une balise distincte pour les serveurs de production et attribuer les adresses IP des serveurs ou du sous-réseau concernés à la balise. Ensuite, dans le Cisco Firepower Threat Defense, vous pourriez autoriser ou bloquer l'accès du réseau d'utilisateurs aux serveurs de production en fonction de la balise. Si vous modifiez ultérieurement les adresses d'hôte ou de réseau associées à la balise dans ISE, vous n'avez pas besoin de modifier la règle de contrôle d'accès définie pour le périphérique Cisco Firepower Threat Defense.

Lorsqu'un périphérique Cisco Firepower Threat Defense évalue la balise SGT comme critère de correspondance de trafic pour une règle de contrôle d'accès, il utilise la priorité suivante :

1. La balise SGT source définie dans le paquet, le cas échéant. Pour que la balise SGT se trouve dans le paquet, les commutateurs et les routeurs du réseau doivent être configurés pour les ajouter. Consultez la documentation ISE pour obtenir des renseignements sur la mise en œuvre de cette méthode.
2. La balise SGT attribuée à la session utilisateur, telle que téléchargée à partir du répertoire de session ISE. Vous devez activer l'option d'écoute des informations de l'annuaire de session pour ce type de correspondance SGT, mais cette option est activée par défaut lorsque vous créez la source d'identité ISE pour la première fois. La balise SGT peut être mise en correspondance avec la source ou la destination. Bien que cela ne soit pas obligatoire, vous devez également configurer normalement une règle d'identité d'authentification passive, en utilisant la source d'identité ISE et un domaine AD, pour recueillir les informations sur l'identité de l'utilisateur.
3. Le mappage SGT-adresse IP téléchargé à l'aide de SXP. Si l'adresse IP se trouve dans la plage d'une SGT, le trafic correspond à la règle de contrôle d'accès qui utilise la SGT. La balise SGT peut être mise en correspondance avec la source ou la destination.

   ISE utilise le protocole SXP (Security-group eXchange Protocol) pour propager la base de données de mappage IP-SGT vers les périphériques réseau. Lorsque vous configurez le périphérique Cisco Firepower Threat Defense pour utiliser un serveur ISE, vous devez activer l'option qui permet d'écouter le sujet SXP provenant d'ISE. Ainsi, le périphérique Cisco Firepower Threat Defense prend connaissance des balises et des mappages du groupe de sécurité directement auprès d'ISE et reçoit une notification chaque fois qu'ISE publie des balises et des mappages de groupe de sécurité mis à jour. Cela garantit que la liste des balises de groupe de sécurité et des mappages reste à jour sur le périphérique, afin que le périphérique Cisco Firepower Threat Defense puisse appliquer efficacement la politique définie dans ISE.

Configurer le contrôle d'accès en fonction de la balise de groupe de sécurité (SGT)

Pour configurer des règles de contrôle d'accès qui utilisent des balises de groupe de sécurité (SGT) comme critères de correspondance, vous devez d'abord configurer le périphérique pour obtenir les mappages SGT d'un serveur ISE.

La procédure suivante explique le processus de bout en bout basé sur l'hypothèse que vous souhaitez obtenir tous les mappages définis dans ISE, y compris les mappages SGT-adresses IP publiés par SXP. Vous pouvez aussi faire comme suit :

- Si vous souhaitez utiliser les informations SGT dans les paquets uniquement, et ne pas utiliser les mappages téléchargés à partir d'ISE, créez simplement des objets dynamiques de groupe SGT et utilisez-les comme critères SGT de source dans les règles de contrôle d'accès. Notez que dans ce cas, vous pouvez utiliser

les balises SGT comme condition de source uniquement; ces balises ne correspondront jamais aux critères de destination.

- Si vous souhaitez utiliser les balises SGT dans les paquets et uniquement les mappages SGT des sessions utilisateur, vous n'avez pas besoin d'activer l'option d'abonnement à la rubrique SXP dans la source d'identité ISE, ni de configurer ISE pour publier des mappages SXP. Vous pouvez utiliser ces informations pour les conditions de correspondance de source et de destination.

Avant de commencer

L'hypothèse ici est que vous avez déjà configuré Cisco TrustSec dans votre réseau et que vous ajoutez simplement l'appareil Cisco Firepower Threat Defense en tant que point d'application de la politique. Si vous n'avez pas déployé Cisco TrustSec, veuillez commencer par ISE et configurer votre réseau, puis revenez à cette procédure. L'explication de Cisco TrustSec n'entre pas dans le cadre de ce document.

Procédure

Étape 1 Assurez-vous que les balises SGT sont définies, qu'ISE est configuré correctement pour publier la rubrique SXP et que tous les mappages statiques nécessaires sont en place.

Consultez Configurer les groupes de sécurité et la publication SXP dans ISE, à la page 39.

Étape 2 Mettez à jour l'objet Identity Services Engine (Moteur de services d'identité) pour être à l'écoute de la rubrique SXP.

Vous pouvez utiliser ISE pour obtenir des mappages SGT de session utilisateur, des mappages SGT statiques d'adresses IP par l'intermédiaire de SXP, ou les deux. Par défaut, lorsque vous configurez la source d'identité ISE, elle obtient uniquement les mappages de sessions utilisateur ; vous devez activer l'option d'écoute de la rubrique SXP depuis ISE.

a) Choisissez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
b) Modifiez l'objet ISE. Si vous n'en avez pas encore configuré, cliquez sur **+** > **Identity Services Engine** (Moteur de services d'identité) et consultez Configurer Identity Services Engine (ISE).
c) Sous **Subscribe To** (S'abonner à), sélectionnez **SXP Topic** (Rubrique SXP).

Assurez-vous que **Session Directory Topic** (Rubrique Session Directory) est également sélectionné si vous utilisez l'authentification passive ou si vous souhaitez des mappages utilisateur-SGT.

d) Cliquez sur **OK**.

Étape 3 Déployez vos modifications et attendez que le système télécharge les balises et les mappages à partir d'ISE.

Après avoir configuré la source d'identité ISE et déployé les modifications, le système récupère les informations de balise de groupe de sécurité (SGT) à partir du serveur ISE. Le téléchargement ne se fera pas avant le déploiement des modifications.

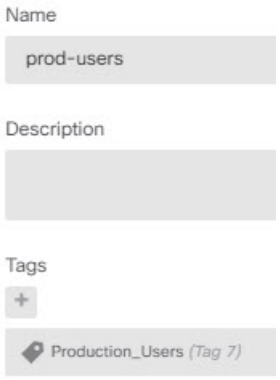
Étape 4 Créez les objets de groupe SGT requis pour vos règles de contrôle d'accès.

Vous ne pouvez pas utiliser les informations extraites d'ISE directement dans une règle de contrôle d'accès. Au lieu de cela, vous devez créer des groupes SGT, qui font référence aux informations SGT téléchargées.

Vos groupes de balises SGT peuvent faire référence à plusieurs SGT, vous pouvez donc appliquer une politique basée sur les collections de balises pertinentes, le cas échéant.

Le nombre et le contenu des objets dépendent des règles de contrôle d'accès que vous avez l'intention d'écrire. Répétez le processus suivant pour créer tous les objets dont vous avez besoin.

a) Choisissez **Objects (Objets)** > **SGT Groups (Groupes SGT)**.
b) Cliquez sur **+** pour ajouter un nouvel objet ou modifier un objet existant.
c) Pour les nouveaux objets, saisissez un nom et éventuellement une description.
d) Sous **Tags (Balises)**, cliquez sur **+** et sélectionnez toutes les balises à inclure dans le groupe.



e) Cliquez sur **OK**.

Étape 5 Créez des règles de contrôle d'accès qui utilisent les objets de groupe SGT.

Par exemple, la règle suivante autorise le trafic des utilisateurs de production vers les serveurs de production. La règle dépend entièrement des balises SGT ; elle n'est pas limitée par l'interface source/destination ni par tout autre critère. Ainsi, la règle s'appliquera dynamiquement au trafic, car il provient de différentes interfaces et à mesure que vous modifierez l'appartenance au groupe de sécurité dans ISE. Si le paquet ne contient pas explicitement de SGT source, la correspondance de source/destination sera basée sur les adresses IP du paquet par rapport aux mappages SGT-adresses IP obtenus à partir des informations de session utilisateur ou des mappages publiés par SXP.

a) Choisissez **Politiques** > **Contrôle d'accès**.
b) Cliquez sur **+** pour créer une nouvelle règle ou modifier une règle existante.
c) Saisissez un nom de règle et sélectionnez **Allow** (Autoriser) comme action.
d) Dans l'onglet **Source/Destination**, cliquez sur **+** sous **Source** > **SGT Groups (Groupes SGT)**, puis sélectionnez l'objet que vous avez créé pour les utilisateurs de production.
e) Dans l'onglet **Source/Destination**, cliquez sur **+** sous **Destination** > **SGT Groups (Groupes SGT)** , et sélectionnez l'objet que vous avez créé pour les serveurs de production.
f) Configurez les autres options selon vos besoins. Par exemple, vous pouvez activer la journalisation et appliquer une politique de prévention des intrusions.
g) Cliquez sur **OK**.

Étape 6 Déployez la configuration.

Configurer les groupes de sécurité et la publication SXP dans ISE

Vous devez effectuer de nombreuses configurations dans Cisco Identity Services Engine (ISE) pour créer la politique TrustSec et les balises de groupes de sécurité (SGT). Veuillez consulter la documentation ISE pour des informations plus complètes sur la mise en œuvre de TrustSec.

La procédure suivante sélectionne les points saillants des paramètres principaux que vous devez configurer dans ISE pour que le périphérique Cisco Firepower Threat Defense puisse télécharger et appliquer les mappages statiques SGT-à-adresse IP, qui peuvent ensuite être utilisés pour la mise en correspondance SGT source et destination dans les règles de contrôle d'accès. Consultez la documentation d'ISE pour obtenir des informations détaillées.

Les captures d'écran de cette procédure sont basées sur ISE 2.4. Les chemins d'accès exacts à ces fonctionnalités pourraient changer dans les versions ultérieures, mais les concepts et les exigences seront les mêmes. Bien que la version 2.4 ou ultérieure d'ISE soit recommandée, de préférence la version 2.6 ou ultérieure, la configuration devrait fonctionner à partir du correctif 1 d'ISE 2.2.

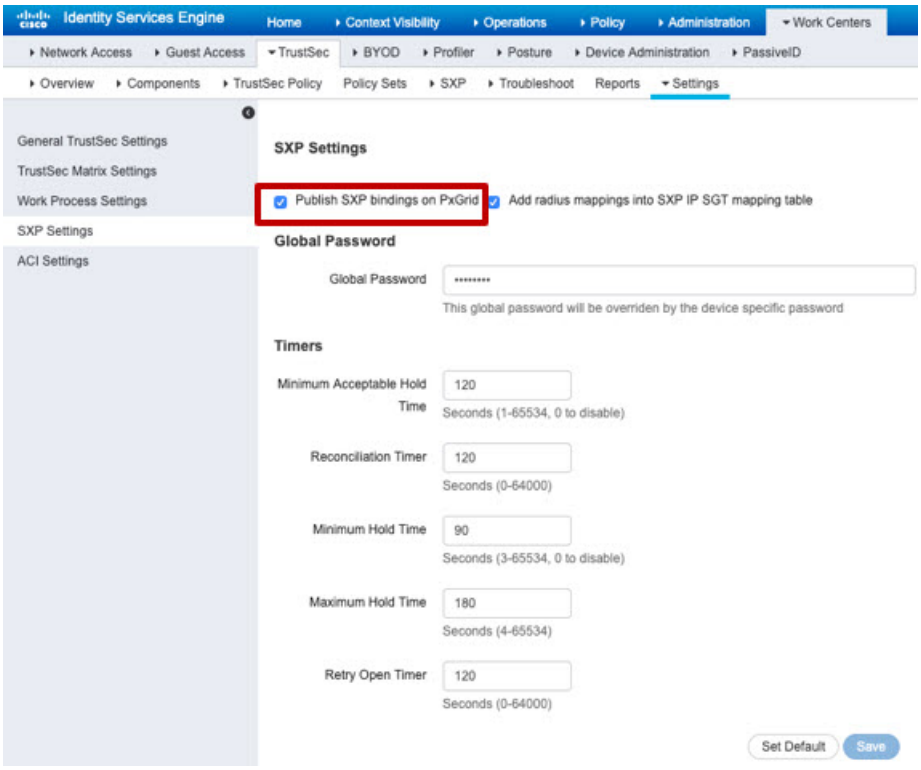
Avant de commencer

Vous devez posséder la licence ISE Plus pour publier les mappages statiques SGT-adresses IP et pour obtenir les mappages utilisateur session-SGT afin que le périphérique Cisco Firepower Threat Defense puisse les recevoir.

Procédure

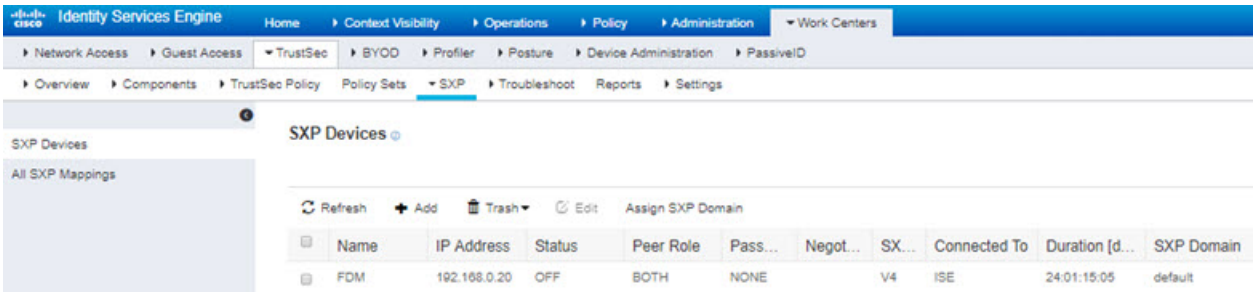
Étape 1 Choisissez **Work Centers** > **TrustSec** > **Settings** > **SXP Settings** > **(paramètres SXP)**, puis sélectionnez l'option **Publish SXP Bindings on PxGrid** (Publier les liens SXP sur PxGrid).

Cette option permet à ISE d'envoyer les mappages SGT à l'aide de SXP. Vous devez sélectionner cette option pour que le périphérique FTD puisse « écouter » n'importe quel élément, de la liste au sujet SXP. Cette option doit être sélectionnée pour que le périphérique FTD reçoive des informations de mappage SGT vers l'adresse IP statique. Ce n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets, ou les balises SGT qui sont attribuées à une session utilisateur.

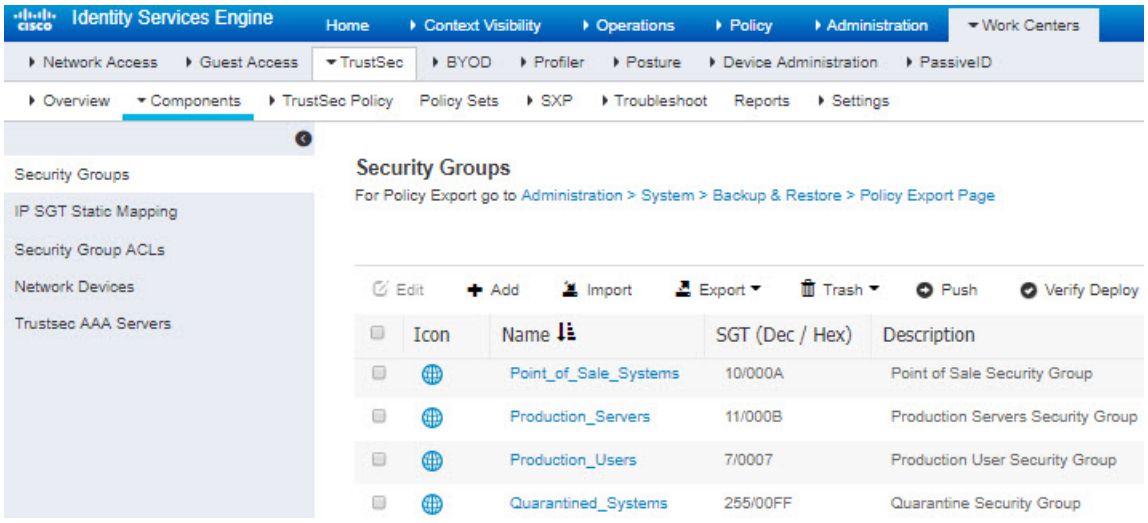


Étape 2 Choisissez **Work Centers** > **TrustSec** > **SXP** > **SXP Devices** (Centres de travail > TrustSec > SXP > Périphériques SXP) et ajoutez un périphérique.

Il n'est pas nécessaire que ce soit un périphérique réel, vous pouvez même utiliser l'adresse IP de gestion du périphérique Cisco Firepower Threat Defense. La table a simplement besoin d'au moins un périphérique pour amener ISE à publier les mappages statiques SGT- vers adresses IP. Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.

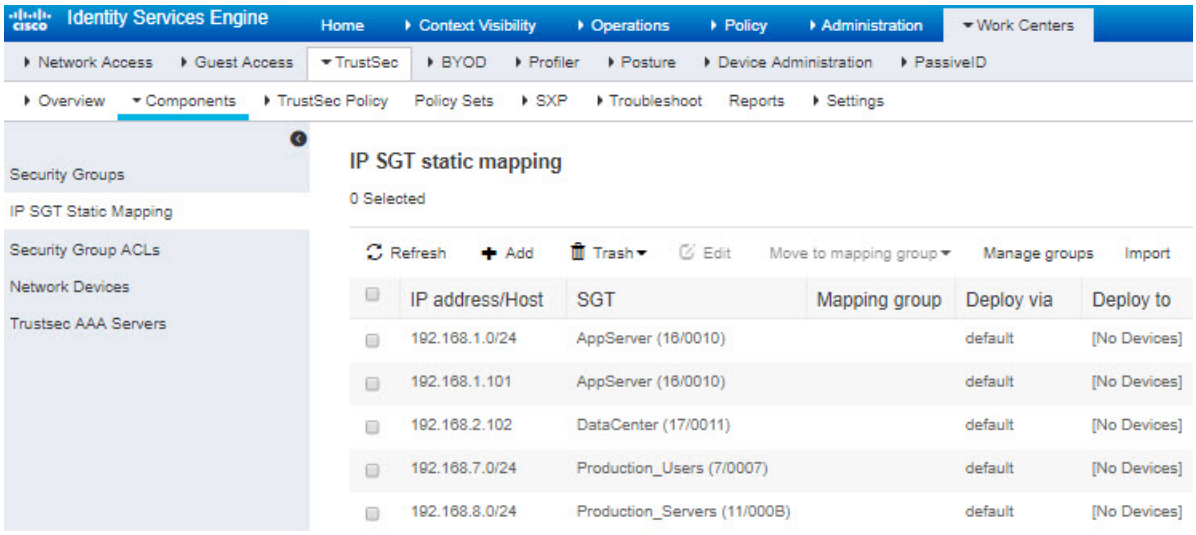


Étape 3 Choisissez **Work Centers** > **TrustSec** > **Components** > **Security Groups** (Centres de travail > TrustSec > Composants > Groupes de sécurité) et vérifiez que des balises de groupes de sécurité sont définies. Créez-en de nouveaux si nécessaire.



Étape 4 Choisissez **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping** (Centres de travail > TrustSec > Composants > Mappage statique SGT IP) et mapper les adresses IP de l'hôte et du réseau aux balises du groupe de sécurité.

Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.



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.