Premiers pas avec les politiques de prévention des intrusions

Les rubriques suivantes expliquent comment démarrer avec les politiques de prévention des intrusions :

Principes de base de la politique de prévention des intrusions

Les *politiques de prévention des intrusions* sont des ensembles définis de configurations de détection et de prévention des intrusions qui inspectent le trafic à la recherche de violations de la sécurité et qui, dans les déploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. Les politiques de prévention des intrusions sont invoquées par votre politique de contrôle d'accès et constituent la dernière ligne de défense du système avant que le trafic ne soit autorisé à atteindre sa destination.

Les règles de prévention des intrusions sont au cœur de chaque politique de prévention des intrusions. Une règle activée oblige le système à générer des incidents d'intrusion pour le trafic correspondant à la règle (et au bloquer éventuellement). La désactivation d'une règle arrête le traitement de la règle.

Le système fournit plusieurs politiques de base de prévention des intrusions qui vous permettent de profiter de l'expérience des Talos Intelligence Group. Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur (activé ou désactivé) et fournit les configurations initiales pour d'autres paramètres avancés.

Astuces Les politiques d'analyse de prévention des intrusions et de réseau fournies par le système portent le même nom, mais contiennent des configurations différentes. Par exemple, la politique d'analyse de réseau équilibrée, sécurité et connectivité, et la politique de prévention des intrusions, sécurité et connectivité équilibrées fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles de prévention des intrusions. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions.

Si vous créez une politique de prévention des intrusions personnalisée, vous pouvez :

- Optimiser la détection en activant et en désactivant les règles, ainsi qu'en écrivant et en ajoutant vos propres règles.
- Utiliser les recommandations de Cisco pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.
- Configurer divers paramètres avancés tels que les alertes externes, le prétraitement des données sensibles et le seuillage des règles globales.
- Utiliser les couches comme composantes de base pour gérer efficacement plusieurs politiques de prévention des intrusions.

Dans un déploiement en ligne, une politique de prévention des intrusions peut bloquer et modifier le trafic :

- *Les règles de suppression* peuvent abandonner les paquets correspondants et générer des incidents d'intrusion. Pour configurer une règle de suppression de prévention des intrusions ou de préprocesseur, définissez son état sur Drop (Abandonner) et Generate Events (générer des événements).
- Les règles de prévention des intrusions peuvent utiliser le mot-clé `replace` pour remplacer du contenu malveillant.

Pour que les règles de prévention des intrusions affectent le trafic, vous devez configurer correctement les règles de suppression et les règles qui remplacent le contenu, et vous devez également déployer correctement les périphériques gérés en ligne, c'est-à-dire avec des ensembles d'interfaces intégrés. Enfin, vous devez activer le *comportement de suppression* de la politique de prévention des intrusions, ou le paramètre **Abandon lorsque en ligne**.

Lorsque vous adaptez votre politique de prévention des intrusions, en particulier lors de l'activation et de l'ajout de règles, gardez à l'esprit que certaines règles de prévention des intrusions exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière. Avant qu'une politique de prévention des intrusions n'examine un paquet, le paquet est prétraité selon les configurations d'une politique d'analyse de réseau. Si vous désactivez un préprocesseur requis, le système l'utilise automatiquement avec ses paramètres actuels, bien que le préprocesseur reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Mise en garde Le prétraitement et l'inspection de prévention des intrusions sont si étroitement liés que les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet **doivent** se compléter mutuellement. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**.

Après avoir configuré une politique de prévention des intrusions personnalisée, vous pouvez l'utiliser dans le cadre de votre configuration de contrôle d'accès en associant la politique de prévention des intrusions à une ou plusieurs règles de contrôle d'accès ou à une action par défaut d'une politique de contrôle d'accès. Cela oblige le système à utiliser la politique de prévention des intrusions pour examiner une partie du trafic autorisé avant que le trafic n'atteigne sa destination finale. Un ensemble de variables que vous associez à la politique de prévention des intrusions vous permet de refléter avec précision votre réseau domestique et externe et, le cas échéant, les serveurs de votre réseau.

Notez que par défaut, le système désactive l'inspection des intrusions 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 pour laquelle l'inspection des intrusions est configurée.

Exigences de licence pour les politiques de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les politiques de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Gestion des politiques de prévention des intrusions

Sur la page Intrusion Policy (politique de prévention des intrusions) (**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**), vous pouvez afficher vos politiques de prévention des intrusions personnalisées actuelles, ainsi que les informations suivantes :

- l'heure et la date de la dernière modification de la politique (en heure locale) et l'utilisateur qui l'a modifiée
- si le paramètre **Abandon quand en ligne** est activé, ce qui vous permet d'abandonner et de modifier le trafic dans un déploiement en ligne. Un déploiement en ligne peut comprendre des configurations déployées sur des périphériques utilisant des interfaces routées, commutées ou transparentes, ou des paires d'interfaces en ligne.
- quelles politiques de contrôle d'accès et quels périphériques utilisent la politique de prévention des intrusions pour inspecter le trafic
- si une politique comporte des modifications non enregistrées, et des informations sur qui (le cas échéant) modifie actuellement la politique
- dans un déploiement multidomaine, le domaine dans lequel la politique a été créée

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

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

Étape 2 Gérez votre politique de prévention des intrusions :

- Comparer : Cliquez sur **Comparer les politiques**; voir Comparer les politiques.
- Create (créer) : Cliquez sur **Create Policy**(créer une politique). voir :
  - Création d'une politique de prévention des intrusions Snort 2 personnalisée, à la page 5 pour les politiques Snort 2
  - *la création d'un sujet de politique de prévention des intrusions Snort 3 personnalisée* dans la dernière version de Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour les politiques Snort 3.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté de la politique que vous souhaitez supprimer. Le système vous demande de confirmer et vous informe si un autre utilisateur a des modifications non enregistrées dans la politique. Cliquez sur **OK** pour confirmer.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.
- Modifier – Choisissez :
  - **Version Snort 2**; Consultez Modification des politiques de prévention des intrusions Snort 2, à la page 6.
  - **Version Snort 3**; Consultez la rubrique *Modification des politiques de prévention des intrusions Snort 3* dans la dernière version de Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

- Exporter : si vous souhaitez exporter une politique de prévention des intrusions pour l'importer sur un autre Cisco Secure Firewall Management Center, cliquez sur **YouTube EDU** ( ); consultez la*Exportation de configurations* dans Guide d'administration Cisco Secure Firewall Management Center.
- Deploy—Choose (déployer, choisir) **Deploy (déployer)** > **Deployment (déploiement)**; voir Déployer les modifications de configuration.
- Rapport : Cliquez sur **Rapport** ( ); voir Générer des rapports sur les politiques appliquées.

Création d'une politique de prévention des intrusions personnalisée

Lorsque vous créez une politique de prévention des intrusions, vous devez lui donner un nom unique, définir une politique de base et définir un comportement d'abandon.

La stratégie de base définit les paramètres par défaut de la stratégie de prévention des intrusions. La modification d'un paramètre dans la nouvelle politique remplace les paramètres de la politique de base, mais ne les change pas. Vous pouvez utiliser une politique fournie par le système ou une politique personnalisée comme politique de base.

Création d'une politique de prévention des intrusions Snort 2 personnalisée

Procédure

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

Étape 2 Cliquez sur **Créer une politique**. Si vous avez des modifications non enregistrées dans une autre politique, cliquez sur **Annuler** lorsque vous êtes invité à revenir à la page Intrusion Policy (politique de prévention des intrusions).

Assurez-vous que l'onglet **Intrusion Policies**(Politiques de prévention des intrusions) est sélectionné.

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 Choisissez le **Mode d'inspection**.

L'action sélectionnée détermine si les règles de prévention des intrusions bloquent et envoient une alerte (mode **prévention**) ou uniquement une alerte (mode **détection**).

Étape 5 Choisissez la **politique de base** initiale.

Vous pouvez utiliser une politique fournie par le système ou une autre politique personnalisée comme politique de base.

Étape 6 Cliquez sur **Save** (enregistrer).

La nouvelle politique a les mêmes paramètres que sa politique de base.

Sujets connexes

Les règles d'intrusion au sein des couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Modification des politiques de prévention des intrusions Snort 2

Procédure

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

Étape 2 Assurez-vous que l'onglet **Intrusion Policies**(Politiques de prévention des intrusions) est sélectionné.

Étape 3 Cliquez sur **Version Snort 2** à côté de la politique de prévention des intrusions que vous souhaitez configurer.

Étape 4 Modifier votre politique

- Modifiez la politique de base (modifier la politique de base) : Choisissez une politique de base dans la liste déroulante **Base Policy** (politique de base); voir Modification de la politique de base en cours.
- Configure advanced settings (configurer les paramètres avancés) : cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation. voir Paramètres avancés de la politique de prévention des intrusions, à la page 10.
- Configurer les règles de prévention des intrusions recommandées par Cisco : cliquez sur **Cisco Recommendations** dans le panneau de navigation. voir Génération et application de recommandations Cisco
- Comportement d'abandon dans un déploiement en ligne : cochez ou décochez la case **Drop when Inline**; voir Définition du comportement d'abandon dans un déploiement en ligne, à la page 9.
- Filtrer les règles par état des règles recommandées : après avoir généré des recommandations, cliquez sur **View** (afficher) à côté de chaque type de recommandation. Cliquez sur **Afficher les modifications recommandées** pour afficher toutes les recommandations.
- Filter Rules by Current Rule state (filtre les règles par l'état actuel des règles) : cliquez sur **View** (afficher) à côté de chaque type d'état de règle (générer des événements, supprimer et générer des événements). voir Filtres de règles d'intrusion dans une politique de prévention des intrusions.
- Manage Policy Layers (gestion des couches des politiques) : Cliquez sur **Policy Layers** (couches des politiques) dans le panneau de navigation. voir Gestion des couches.
- Manage intrusion Rules (gestion des règles de prévention des intrusions) : cliquez sur **Manage Rules** (gestion des règles) ; voir Affichage des règles d'intrusion dans une politique d'intrusion.
- Afficher les paramètres de la politique de base : Cliquez sur **Gérer la politique de base**; voir La couche de base.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, sélectionnez **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Génération et application de recommandations Cisco
Configuration des règles d'intrusion dans les couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Modifications des politiques de prévention des intrusions

Lorsque vous créez une politique de prévention des intrusions, elle a les mêmes règles de prévention des intrusions et paramètres avancés que sa politique de base.

Le système met en cache une politique de prévention des intrusions par utilisateur. Lors de la modification d'une politique de prévention des intrusions, si vous choisissez un menu ou un autre chemin vers une autre page, vos modifications restent dans le cache système même si vous quittez la page.

Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions

Une politique de contrôle d'accès peut avoir plusieurs règles de contrôle d'accès associées à des politiques de prévention des intrusions. Vous pouvez configurer l'inspection de prévention des intrusions pour toute règle de contrôle d'accès Allow (autorisation) ou Interactive Block (blocage interactif), ce qui vous permet de faire correspondre différents profils d'inspection des intrusions avec différents types de trafic sur votre réseau avant qu'il n'atteigne sa destination finale.

Chaque fois que le système utilise une politique de prévention des intrusions pour évaluer le trafic, il utilise un *ensemble de variables* associé. La plupart des variables d'un ensemble représentent des valeurs couramment utilisées dans les règles de prévention des intrusions pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles et de règles dynamiques.

Astuces Même si vous utilisez les politiques de prévention des intrusions fournies par le système, Cisco vous recommande **fortement** de configurer les variables du système relatives aux intrusions pour refléter avec exactitude votre environnement réseau. Au minimum, modifiez les variables par défaut dans l'ensemble par défaut.

Comprendre les politiques de prévention des intrusions fournies par le système et personnalisées

Cisco fournit plusieurs politiques de prévention des intrusions avec le système. En utilisant les politiques de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience de Talos Intelligence Group. Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur, et fournit les configurations initiales pour les paramètres avancés. Vous pouvez utiliser les politiques fournies par le système telles quelles ou vous pouvez les utiliser comme base pour des politiques personnalisées. L'élaboration de politiques personnalisées peut améliorer les performances du système dans votre environnement

et fournir un aperçu plus précis du trafic malveillant et des violations de politiques qui se produisent sur votre réseau.

Journalisation des événements de connexion et d'intrusion

Lorsqu'une politique de prévention des intrusions appelée par une règle de contrôle d'accès détecte une intrusion et génère un incident d'intrusion, elle enregistre cet événement dans Cisco Secure Firewall Management Center. Le système consigne également automatiquement la fin de la connexion où l'intrusion s'est produite dans la base de données Cisco Secure Firewall Management Center, quelle que soit la configuration de journalisation de la règle de contrôle d'accès.

Sujets connexes

Variables prédéfinies par défaut

Configuration des règles de contrôle d'accès et politiques de prévention des intrusions

Le nombre de politiques de prévention des intrusions uniques que vous pouvez utiliser dans une seule politique de contrôle d'accès dépend du modèle des machines cibles; des périphériques plus puissants peuvent en gérer plus. Chaque **paire** de politique de prévention des intrusions et d'ensemble de variables compte pour une politique. Bien que vous puissiez associer une paire d'ensembles de variables de politique de prévention des intrusions différente à chaque règle d'autorisation et de blocage interactif (ainsi qu'à l'action par défaut), vous ne pouvez pas déployer de politique de contrôle d'accès si les machines cibles disposent de ressources insuffisantes pour effectuer l'inspection configurée.

Configuration d'une règle de contrôle d'accès pour la prévention des intrusions

Vous devez être un administrateur, un administrateur de l'accès ou un administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, créez une règle ou modifiez une règle existante; voir Composants des règles de contrôle d'accès.

Étape 2 Assurez-vous que l'action de règle est définie sur **Allow**(autorisation), **Interactive Block** (blocage interactif) ou **Interactive Block with reset (blocage interactif) avec réinitialisation**.

Étape 3 Cliquez sur **Inspection**.

Étape 4 Choisissez une **politique de prévention des intrusions** fournie par le système ou personnalisée, ou choisissez **Aucun** pour désactiver l'inspection de prévention des intrusions pour le trafic qui correspond à la règle de contrôle d'accès.

Étape 5 Si vous souhaitez modifier l'ensemble de variables associé à la politique de prévention des intrusions, choisissez une valeur dans la liste déroulante **Ensemble de variables**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la règle.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Ensemble de variables
Scénarios de redémarrage de Snort

Comportement d'abandon dans un déploiement en ligne

Si vous souhaitez évaluer comment votre configuration fonctionnerait dans un déploiement en ligne (c'est-à-dire où les configurations pertinentes sont déployées sur des périphériques utilisant des interfaces routées, commutées ou transparentes, ou des paires d'interfaces en ligne) sans réellement affecter le trafic, vous pouvez désactiver le comportement d'abandon. Dans ce cas, le système génère des incidents d'intrusion mais ne supprime pas les paquets qui déclenchent les règles d'abandon. Lorsque vous êtes satisfait des résultats, vous pouvez activer le comportement d'abandon.

Notez que dans les déploiements passifs ou en ligne en mode Tap, le système ne peut pas affecter le trafic, quel que soit le comportement d'abandon. Dans un déploiement passif, les règles définies sur **Drop et Generate Events** (Abandonner et générer des événements) se comportent de la même manière que les règles définies sur **Generate Events** (Générer des événements). Le système génère des incidents d'intrusion, mais ne peut pas abandonner de paquets.

Remarque Supposons qu'une action de blocage de fichier entraîne un verdict de politique de fichier bloqué ou en attente sur un paquet, et que ultérieurement, un événement IPS est généré sur le même paquet. Dans ce cas, l'événement IPS est marqué comme Abandonné au lieu de Aurait été abandonné, même si la politique IPS est en mode de détection (IDS).

Remarque Pour bloquer le transfert de programmes malveillants sur FTP, vous devez non seulement configurer correctement Défense contre les programmes malveillants , mais aussi activer l'option **Abandon lorsque en ligne** dans la politique de prévention des intrusions par défaut de votre politique de contrôle d'accès.

Lorsque vous affichez les incidents d'intrusion, les flux de travail peuvent inclure le *résultat en ligne*, qui indique si le trafic a été réellement abandonné ou s'il aurait été abandonné.

Définition du comportement d'abandon dans un déploiement en ligne

Procédure

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

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Définissez le comportement de suppression de la politique :

- Cochez la case **Drop if Inline** (Abandonner quand en ligne) pour permettre aux règles de prévention des intrusions d'affecter le trafic et de générer des événements.
- Décochez la case **Abandonner quand en ligne** pour empêcher les règles de prévention des intrusions d'affecter le trafic tout en générant des événements.

Étape 4 Cliquez sur **Commit Changes** (valider les modifications) pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique.

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Comportement d'abandon dans un déploiement de système double

Lorsque deux systèmes sont connectés ensemble dans un réseau, il est normal de voir le premier système abandonner des événements tout en enregistrant un événement d'abandon ou d'abandon potentiel sur le second système. Le premier système décide d'abandonner les paquets avant d'analyser le dernier paquet du fichier, tandis que le deuxième système enquête également et identifie le trafic comme « à abandonner ».

Par exemple, une requête HTTP GET de 5 paquets dont le premier paquet déclenche une règle est bloquée par le premier système et seul le dernier paquet est abandonné. Le deuxième système reçoit seulement 4 paquets et la connexion est abandonnée, mais lorsque le deuxième système purge finalement la demande GET partielle pendant qu'il élague la session, il déclenche la même règle avec « aurait abandonné » comme résultat en ligne.

Paramètres avancés de la politique de prévention des intrusions

Les *paramètres avancés* d'une politique de prévention des intrusions nécessitent une expertise particulière pour être configurés. La politique de base de votre politique de prévention des intrusions détermine les paramètres avancés activés par défaut et la configuration par défaut de chacun.

Lorsque vous choisissez **Advanced Settings** (paramètres avancés) dans le panneau de navigation d'une politique de prévention des intrusions, la politique répertorie ses paramètres avancés par type. Dans la page Advanced Settings (paramètres avancés), vous pouvez activer ou désactiver les paramètres avancés dans votre politique de prévention des intrusions, et accéder aux pages de configuration des paramètres avancés. Un paramètre avancé doit être activé pour que vous puissiez le configurer.

Lorsque vous désactivez un paramètre avancé, le sous-lien et le lien de **modification** ne s'affichent plus, mais vos configurations sont conservées. Notez que certaines configurations de politiques de prévention des intrusions (règles de données sensibles, alertes SNMP pour les règles de prévention des intrusions) nécessitent des paramètres avancés activés et correctement configurés.

La modification de la configuration d'un paramètre avancé nécessite une compréhension de la configuration que vous modifiez et de son impact potentiel sur votre réseau.

Détection des menaces spécifiques

Le préprocesseur des données sensibles détecte les données sensibles telles que les numéros de cartes de crédit et les numéros de sécurité sociale dans le texte ASCII.

Notez que d'autres préprocesseurs qui détectent des menaces spécifiques (attaques par orifice arrière, plusieurs types de balayage de ports et attaques basées sur le débit qui tentent de submerger votre réseau avec un trafic excessif) sont configurés dans les politiques d'analyse de réseau.

Seuils de règles d'intrusion

Le seuillage de règles globales peut éviter que votre système ne soit submergé par un grand nombre d'événements en vous permettant d'utiliser des seuils pour limiter le nombre de fois que le système consigne et affiche les incidents d'intrusion.

Réponses externes

En plus des différentes affichages des incidents d'intrusion dans l'interface Web, vous pouvez activer la journalisation dans le journal système (syslog) ou envoyer des données d'événements à un serveur de déroutement SNMP. Par politique, vous pouvez préciser les limites de notification d'incidents d'intrusion, configurer la notification d'incidents d'intrusion aux installations de journalisation externes et configurer les réponses externes aux incidents d'intrusion.

Notez qu'en plus de ces configurations d'alertes par politique, vous pouvez activer ou désactiver globalement les alertes par courriel sur les incidents d'intrusion pour chaque règle ou groupe de règles. Les paramètres de vos alertes par courriel sont utilisés, quelles que soient la politique de prévention des intrusions qui traite un paquet.

Sujets connexes

Principes de base de la détection des données sensibles

Principes de base des seuils de règle globale

Optimisation des performances de détection et de prévention des intrusions

Si vous souhaitez que le système Firepower effectue la détection et la prévention des intrusions, mais que vous n'avez pas besoin de tirer parti des données de découverte, vous pouvez optimiser les performances en désactivant la nouvelle découverte comme décrit ci-dessous.

Avant de commencer

Pour effectuer cette tâche, vous devez avoir l'un des rôles d'utilisateur suivants :

- Administrateur, administrateur d'accès ou administrateur de réseau pour le contrôle d'accès.
- Administrateur ou administrateur de découverte pour la découverte de réseau.

Procédure

Étape 1 Modifiez ou supprimez les règles associées à la politique de contrôle d'accès déployée sur le périphérique cible. Aucune des règles de contrôle d'accès associées à ce périphérique ne peut avoir de conditions d'utilisateur, d'application ou d'URL; voir Créer et modifier les règles de contrôle d'accès.

Étape 2 Supprimez toutes les règles de la politique de découverte de réseau pour le périphérique cible. voir Configuration des règles de découverte du réseau.

Étape 3 Déployez la configuration modifiée sur le périphérique cible; voir Déployer les modifications de configuration.

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.