Premiers pas avec les politiques de prévention des intrusions Snort 3

Ce chapitre fournit des informations sur la gestion des politiques de prévention des intrusions de Snort 3 et la configuration des règles de contrôle d'accès pour la détection et la prévention des intrusions.

Présentation des politiques 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 en matière de prévention des intrusions, qui vous permettent de profiter de l'expérience de Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de l'inspecteur (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.
- Utilisez les recommandations de Cisco Secure Firewall 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.

Une politique de prévention des intrusions peut abandonner les paquets correspondants et générer des incidents d'intrusion. Pour configurer une règle de prévention des intrusions ou d'abandon de préprocesseur, définissez son état sur Block (Bloquer).

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 inspecteur obligatoire, le système l'utilise automatiquement avec ses paramètres actuels, bien que l'inspecteur 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.

Consultez la vidéo pour obtenir de l'aide et des informations supplémentaires concernant la présentation de la politique de prévention des intrusions de Snort 3.

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Création d'une politique de prévention des intrusions Snort 3 personnalisée

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur **Créer une politique**.

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**).

Remarque
Avant de sélectionner le mode de prévention, vous pouvez souhaiter que les règles de blocage déclenchent uniquement une alerte afin de pouvoir identifier les règles qui provoquent de nombreux faux positifs.

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

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

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

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

Prochaine étape

Pour personnaliser la politique, consultez Modification des politiques de prévention des intrusions Snort 3, à la page 4.

Modification des politiques de prévention des intrusions Snort 3

Lors de la modification d'une politique Snort 3, toutes les modifications sont enregistrées instantanément. Aucune action supplémentaire n'est requise pour enregistrer les modifications.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Journalisation des actions liées aux règles

À partir de la version Centre de gestion 7.2.0 , sur la page **Intrusion Events** (Événements d'intrusion), l'événement dans la colonne **Inline Result** (Résultat en ligne) affiche le même nom que l'action IPS appliquée à la règle, afin que vous puissiez voir l'action qui a été appliquée au trafic correspondant à la règle.

Pour les actions IPS, le tableau suivant présente les événements affichés dans la colonne **Inline Result** de la page **Intrusion Events** et dans la colonne **Action** pour **Intrusion Event Type** (type d'incident d'intrusion dans la page **Unified Events** (Événements unifiés).

Action IPS pour Snort 3	Résultat en ligne : Centre de gestion 7.1.0 ou versions antérieures	Résultat en ligne : Centre de gestion 7.2.0 et versions ultérieures
Alerte	Réussite	Alerte
Bloquer	Abandonné/aurait dû être abandonné/partiellement abandonné	Bloquer/bloquerait/blocage partiel
Abandonner	Abandonné/aurait abandonné	Abandon/Abandonnerait
Rejeter	Abandonné/aurait abandonné	Rejeter/rejetterait
Réécrire	Autoriser	Réécrire

Important

- Dans le cas d'une règle sans l'option « Replace » (Remplacer), l'action **Rewrite** (Réécriture) est affichée comme « **Wait Rewrite** » (En attente de réécriture).
- L'action de **réécriture** serait également affichée sous la forme **Would rewrite (réécrirait)** si l'option « Replace » est spécifiée, mais que la politique IPS est en mode de détection ou que le périphérique est en mode TAP en ligne/passif.

Remarque

En cas de compatibilité ascendante (Centre de gestion 7.2.0 assurant la gestion d'un périphérique Threat Defense 7.1.0), les événements mentionnés s'appliquent uniquement à l'action Alert IPS (Alerter IPS) (où la mention **Pass** (Réussite) est affichée comme **Alerte** pour les événements. Pour toutes les autres actions, les événements de Centre de gestion 7.1.0 s'appliquent.

Modifier la politique de base d'une politique de prévention des intrusions

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

Vous pouvez enchaîner jusqu'à cinq politiques personnalisées, quatre d'entre elles utilisant comme politique de base l'une des quatre autres politiques créées précédemment; la cinquième doit utiliser comme base une politique fournie par le système.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur **Modifier** ( ) à côté de la politique de prévention des intrusions que vous souhaitez configurer.

Étape 3 Choisissez une politique dans la liste déroulante **Base Policy** (politique de base).

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Gérer les politiques de prévention des intrusions

Sur la page de prévention des intrusions (**Policies** > **Intrusion**), vous pouvez afficher vos politiques de prévention des intrusions personnalisées actuelles, ainsi que les informations suivantes :

- Nombre de politiques de contrôle d'accès et de périphériques utilisant la politique de prévention des intrusions pour inspecter le trafic
- 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 **Politiques** > **Intrusion**.

Étape 2 Gérez votre politique de prévention des intrusions :

- Create (créer) : cliquez sur **Create Policy**(créer une politique). voir Création d'une politique de prévention des intrusions Snort 3 personnalisée , à la page 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.

- Modifiez les détails de la politique de prévention des intrusions – Cliquez sur **Modifier** ( ) à côté de la politique que vous souhaitez modifier. Vous pouvez modifier le **nom**, le **mode d'inspection** et la **politique de base** de la politique de prévention des intrusions.

- Modifiez les paramètres de politique de prévention des intrusions : cliquez sur **Snort 3 Version** (version Snort 3); voir Modification des politiques de prévention des intrusions Snort 3, à la page 4.

- Exporter : si vous souhaitez exporter une politique de prévention des intrusions pour l'importer sur un autre centre de gestion, cliquez sur Exporter; Reportez-vous à la rubrique *Exportation des configurations* dans la dernière version du Guide de configuration de Cisco Firepower Management Center*Guide de configuration Cisco Secure Firewall Management Center*.

- Deploy (déployer) : choisissez **Deploy** > **Deployment**(déployer > déploiement); voir Déployer les modifications de configuration.

- Report (Rapport) : cliquez sur **Report**(Rapport). ; Consultez la rubrique *Génération des rapports sur les politiques actuelles* dans la dernière version du *Guide de configuration de Cisco Secure Firewall Management Center*. Génère deux rapports, un pour chaque version de politique.

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 du Cisco Talos Intelligence Group (Talos). 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 le centre de gestion (Management Center). Le système consigne également automatiquement la fin de la connexion où l'intrusion s'est produite dans la base de données du centre de gestion, quelle que soit la configuration de journalisation de la règle de contrôle d'accès.

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.

Configurer une règle de contrôle d'accès pour effectuer 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; Consultez la rubrique *Composants de la règle de contrôle d'accès* dans la dernière version du *Guide de configuration de Cisco Secure Firewall Management Center*.

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

Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Déployer les modifications de configuration

Après avoir modifié les configurations, déployez-les sur les appareils ciblés.

Remarque Cette rubrique couvre les étapes de base du déploiement des modifications de configuration. Nous vous recommandons *fortement* de consulter la rubrique sur le *déploiement des modifications de configuration* dans la dernière version du *Guide de configuration Cisco Secure Firewall Management Center* pour comprendre les conditions préalables et les conséquences du déploiement des modifications avant de poursuivre les étapes.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic.

Procédure

Étape 1 Dans la barre de menus Cisco Secure Firewall Management Center, cliquez sur **Deploy** (déployer) puis sélectionnez **Deployment** (déploiement).

La page de GUI répertorie les périphériques dont les configurations sont obsolètes et dont l'état est en **attente**.

- La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets. En développant la liste des appareils, vous pouvez afficher les utilisateurs qui ont modifié les politiques par rapport à chaque liste de politiques.

  Remarque
  Les noms d'utilisateur ne sont pas fournis pour les politiques et objets supprimés.

- La colonne **Inspect Interruption** (inspecter l'interruption) indique si une interruption de l'inspection du trafic peut se produire dans le périphérique pendant le déploiement.

  Si cette colonne est vide pour un périphérique, cela signifie qu'il n'y aura pas d'interruption de l'inspection du trafic sur ce périphérique pendant le déploiement.

- La colonne **Last Modified Time** (heure de la dernière modification) indique la dernière fois que vous avez modifié la configuration.
- La colonne **Preview** (aperçu) vous permet de prévisualiser les modifications pour le prochain déploiement.
- La colonne **Status** (état) indique l'état de chaque déploiement.

Étape 2 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Search (rechercher) : faites une recherche par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Expand (développer) : cliquez sur **Flèche Développer** ( ) pour afficher les modifications de configuration propres au périphérique à déployer.

  Lorsque vous cochez une case à côté d'un périphérique, toutes les modifications apportées au périphérique et répertoriées sous ce dernier sont transmises pour déploiement. Cependant, vous pouvez utiliser **Sélection de politique** ( ) pour sélectionner des politiques ou des configurations spécifiques à déployer tout en conservant les modifications restantes sans les déployer.

  Remarque
  - Lorsque l'état de la colonne **Inspect Interruption** (interruption de l'inspection) indique (**Yes** (oui)) que le déploiement interrompra l'inspection, et peut-être le trafic, sur un appareil Threat Defense, la liste étendue indique les configurations particulières causant l'interruption avec **Inspecter l'interruption** ( ).
  - Lorsque des changements sont apportés aux groupes d'interface, aux zones de sécurité ou aux objets, les appareils touchés sont affichés comme étant périmés sur centre de gestion. Pour vous assurer que ces modifications prennent effet, les politiques relatives à ces groupes d'interface, zones de sécurité ou objets doivent également être déployées avec les modifications. Les politiques concernées sont indiquées comme étant obsolètes sur la page **Prévisualisation** de centre de gestion.

Étape 3 Cliquez sur **Deploy** (déployer).

Étape 4 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Vous avez les choix suivants :

- Deploy (déployer) : Continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Close (fermer) : Quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

Prochaine étape

Pendant le déploiement, en cas d'échec du déploiement pour quelque raison que ce soit, il est possible que l'échec influe sur le trafic. Cependant, cela dépend de certaines conditions. S'il y a certains changements de configuration dans le déploiement, l'échec du déploiement peut entraîner une interruption du trafic. Pour en savoir plus, consultez la rubrique sur le déploiement des modifications de la dernière version du *Guide configuration de Cisco Secure Firewall Management Center*.

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.