Stratégies de prévention des intrusions

Les rubriques suivantes expliquent les politiques de prévention des intrusions et les politiques d'analyse de réseau (Network Analysis Policy, NAP) associées. Les politiques de prévention des intrusions comprennent des règles qui vérifient le trafic pour détecter les menaces et bloquent le trafic qui semble être une attaque. Les politiques d'analyse de réseau contrôlent le prétraitement du trafic, qui prépare le trafic à une inspection plus approfondie en le normalisant et en relevant les anomalies de protocole.

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.

À propos des politiques d'analyse de réseau et de prévention des intrusions

Les politiques d'analyse de réseau et de prévention des intrusions fonctionnent ensemble dans le cadre de la fonction de détection et de prévention des intrusions.

- Une politique d'analyse de réseau régit la façon dont le trafic est décodé et prétraité afin qu'il puisse être évalué de manière plus approfondie, en particulier pour détecter un trafic anormal qui pourrait signaler une tentative d'intrusion.
- Une politique de prévention des intrusions utilise des règles d'intrusion et de préprocesseur (parfois appelées collectivement règles de prévention des intrusions) pour examiner les paquets décodés à la recherche d'attaques basées sur des modèles. Les règles peuvent soit bloquer (abandon) le trafic menaçant et générer un événement, soit simplement le détecter (alerte) et générer uniquement un événement.

Pendant que le système analyse le trafic, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions. Ensemble, les politiques d'analyse de réseau et de prévention des intrusions permettent une inspection large et approfondie des paquets. Elles peuvent vous aider à détecter le trafic réseau, à vous alerter et à vous protéger contre le trafic réseau qui pourrait menacer la disponibilité, l'intégrité et la confidentialité des hôtes et de leurs données.

Politiques d'analyse de réseau et de prévention des intrusions définies par le système

Le système comprend plusieurs paires de politiques d'analyse de réseau et de prévention des intrusions du même nom, qui se complètent et fonctionnent ensemble. Par exemple, il existe des politiques de Politique d'analyse de réseau (NAP) et de prévention des intrusions nommées « Balanced Security and Connectivity », qui sont destinées à être utilisées ensemble. Les politiques fournies par le système sont configurées par 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 préprocesseurs et d'autres paramètres avancés.

À mesure que de nouvelles vulnérabilités sont connues, Talos publie des mises à jour des règles de prévention des intrusions. Ces mises à jour de règles peuvent modifier toute analyse de réseau ou politique de prévention des intrusions fournie par le système, ainsi que des règles de prévention des intrusions et de préprocesseurs nouvelles ou mises à jour, des états modifiés pour les règles existantes et des paramètres de politique par défaut modifiés. Les mises à jour de règles peuvent également supprimer des règles des politiques fournies par le système et fournir de nouvelles catégories de règles, ainsi que modifier l'ensemble de variables par défaut.

Vous pouvez mettre à jour manuellement la base de données de règles ou configurer un calendrier de mise à jour réguliers. Vous devez redéployer une politique mise à jour pour que ses modifications prennent effet. Pour en savoir plus sur la mise à jour des bases de données du système, consultez Mise à jour des bases de données du système..

Voici les politiques fournies par le système :

Politiques d'analyse des intrusions et de sécurité et de connectivité équilibrées

Ces politiques sont conçues pour la vitesse et la détection. Utilisés ensemble, ils constituent un bon point de départ pour la plupart des organisations et des types de déploiement. Au départ, la politique d'analyse de réseau « Balanced Security and Connectivity » fournie par le système est la politique par défaut.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les organisations où la connectivité (permission d'accéder à toutes les ressources) prime sur la sécurité de l'infrastructure réseau. La politique de prévention des intrusions active beaucoup moins de règles que celles activées dans la politique de sécurité avant la connectivité. Seules les règles les plus critiques qui bloquent le trafic sont activées.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les réseaux où la sécurité de l'infrastructure réseau prime sur la facilité d'utilisation. La politique de prévention des intrusions permet d'appliquer de nombreuses règles de prévention des anomalies du réseau qui peuvent alerter sur le trafic légitime ou l'interrompre.

Politiques d'analyse de réseau et de prévention des intrusions

Ces politiques sont conçues pour les réseaux où la sécurité de l'infrastructure du réseau est encore plus importante que celle des politiques de sécurité sur la connectivité, avec un potentiel d'impact opérationnel encore plus grand. Par exemple, la politique de prévention des intrusions active des règles dans un grand

nombre de catégories de menaces, y compris les programmes malveillants, les trousses d'exploit, les vulnérabilités anciennes et courantes, et les exploits connus et répandus.

Mode d'inspection : prévention ou détection

Par défaut, toutes les politiques de prévention des intrusions fonctionnent en mode de prévention pour mettre en œuvre un système de prévention des intrusions (IPS). En mode d'inspection de prévention, si une connexion correspond à une règle de prévention des intrusions dont l'action est d'abandonner le trafic, la connexion est activement bloquée.

Si vous souhaitez plutôt tester l'effet de la politique de prévention des intrusions sur votre réseau, vous pouvez passer au mode de détection, qui implémente un système de détection des intrusions (IDS). Dans ce mode d'inspection, les règles de rejet sont traitées comme des règles d'alerte, où vous êtes informé des connexions correspondantes, mais le résultat de l'action devient aurait bloqué, et les connexions ne sont jamais bloquées.

Vous modifiez le mode d'inspection par politique de prévention des intrusions, de sorte que vous pouvez avoir une combinaison de prévention et de détection.

La politique d'analyse de réseau (Politique d'analyse de réseau (NAP)) Snort 3 dispose également d'un mode d'inspection. Contrairement à la politique d'intrusion, la politique NAP est globale, vous devez donc exécuter tout le traitement NAP en mode de prévention ou de détection. Vous devez utiliser le même mode que vous utilisez pour vos politiques d'intrusion. Si vous avez une combinaison de politiques de prévention et de détection, sélectionnez Prévention pour faire correspondre vos politiques d'intrusion les plus restrictives.

Règles de prévention des intrusions et de préprocesseur

Une règle de prévention des intrusions est un ensemble précis de mots-clés et d'arguments que le système utilise pour détecter les tentatives d'exploitation des vulnérabilités de votre réseau. Lorsque le système analyse le trafic réseau, il compare les paquets aux conditions spécifiées dans chaque règle et déclenche la règle si le paquet de données répond à toutes les conditions spécifiées dans cette dernière.

Le système comprend les types de règles suivants, créés par Cisco Talos Intelligence Group (Talos) :

- Règles de prévention des intrusions, subdivisées en règles d'objets partagés et en règles de texte standard
- Règles de préprocesseur, associées aux préprocesseurs et aux options de détection du décodeur de paquets dans la politique d'analyse de réseau. La plupart des règles de préprocesseur sont désactivées par défaut.

Les rubriques suivantes expliquent en détail les règles d'intrusion.

Attributs des règles d'intrusion

Lorsque vous affichez une politique de prévention des intrusions, vous voyez une liste de toutes les règles de prévention des intrusions disponibles pour identifier les menaces.

La liste de règles pour chaque politique est la même. La différence réside dans l'action configurée pour chaque règle. Comme il y a plus de 30 000 règles, le fait de faire défiler la liste prendra un certain temps. Les règles sont affichées à mesure que vous faites défiler la liste.

Voici les attributs qui définissent chaque règle :

> (Signature Description – Description de la signature)

Cliquez sur le bouton > dans la colonne de gauche pour ouvrir la description de la signature. La description est le code réel utilisé par le moteur d'inspection Snort pour faire correspondre le trafic à la règle.

L'explication du code n'entre pas dans le cadre de ce document, mais il est expliquée en détail dans *le Guide de configuration du centre de gestion* ; sélectionnez le livre pour la version de votre logiciel dans http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html. Recherchez des informations sur la modification des règles de prévention des intrusions.

Les signatures contiennent des variables pour certains éléments. Pour en savoir plus, consultez Ensemble de variables d'intrusion par défaut, à la page 4.

GID

Identifiants de générateur (ID). Ce nombre indique quel composant du système évalue la règle et génère des événements. Un 1 indique une règle de prévention des intrusions de texte standard et un 3 indique une règle de prévention des intrusions d'objets partagés. (La différence entre ces types de règles n'est pas significative pour un utilisateur FDM.) Il s'agit des principales règles d'intérêt lors de la configuration d'une politique de prévention des intrusions. Pour plus d'informations sur les autres GID, consultez Identifiants du Générateur, à la page 5.

SID

Identifiant (ID) Snort, également appelé ID de signature. Les ID Snort inférieurs à 1 000 000 ont été créés par Cisco Talos Intelligence Group (Talos).

Action

L'état de cette règle dans la politique de prévention des intrusions sélectionnée. Pour chaque règle, « (Default) » est ajouté à l'action qui est l'action par défaut pour la règle dans cette politique. Pour rétablir une règle à son paramètre par défaut, sélectionnez cette action. Les actions possibles sont :

- **Alert** (Alerte) : ce choix crée un événement lorsque cette règle correspond au trafic, sans interrompre la connexion.
- **Drop** (Abandon) : ce choix crée un événement lorsque cette règle correspond au trafic et interrompt également la connexion.
- **Disabled** (Désactivé) : ne fait pas correspondre le trafic à cette règle. Aucun événement n'est généré.

État

Pour les règles Snort 2, l'état est une colonne distincte. Si vous modifiez l'action par défaut d'une règle, cette colonne affiche « Overridden » (Remplacé). Sinon, la colonne est vide.

Pour les règles Snort 3, l'état « Overridden » (Remplacé) s'affiche au bas de l'attribut Action, si vous l'avez modifié.

Message

Il s'agit du nom de la règle, qui apparaît également dans les événements déclenchés par la règle. Le message identifie généralement la menace à laquelle la signature correspond. Vous pouvez effectuer une recherche sur Internet pour obtenir plus d'informations sur chaque menace.

Ensemble de variables d'intrusion par défaut

Les signatures des règles de prévention des intrusions contiennent des variables pour certains éléments. Voici les valeurs par défaut pour les variables, $HOME_NET et $EXTERNAL_NET étant les variables les plus couramment utilisées. Notez que le protocole est spécifié séparément des numéros de port, donc les variables de port sont des numéros uniquement.

- $DNS_SERVERS = $HOME_NET (signifie toute adresse IP).

- $EXTERNAL_NET = toute adresse IP.
- $FILE_DATA_PORTS = $HTTP_PORTS, 143, 110.
- $FTP_PORTS = 21, 2100, 3535.
- $GTP_PORTS = 3386, 2123, 2152.
- $HOME_NET = toute adresse IP.
- $HTTP_PORTS = 144 ports numérotés : 36, 80-90, 311, 383, 443, 555, 591, 593, 631, 666, 801, 808, 818, 901, 972, 1158, 1212, 1220, 1414, 1422, 1533, 1741, 1830, 1942, 2231, 2301, 2381, 2578, 2809, 2980, 3029, 3037, 3057, 3128, 3443, 3507, 3702, 4000, 4343, 4848, 5000, 5117, 5222, 5250, 5450, 5600, 5814, 6080, 6173, 6767, 6988, 7000, 7001, 7005, 7071, 7080, 7144, 7145, 7510, 7770, 7777-7779, 8000, 8001, 8008, 8014, 8015, 8020, 8028, 8040, 8060, 8080-8082, 8085, 8088, 8118, 8123, 8161, 8180-8182, 8222, 8243, 8280, 8300, 8333, 8344, 8400, 8443, 8500, 8509, 8787, 8800, 8888, 8899, 8983, 9000, 9002, 9060, 9080, 9090, 9091, 9111, 9290, 9443, 9447, 9710, 9788, 9999, 10000, 11371, 12601, 13014, 15489, 19980, 23472, 29991, 33300, 34412, 34443, 34444, 40007, 41080, 44449, 50000, 50002, 51423, 53331, 55252, 55555, 56712.
- $HTTP_SERVERS = $HOME_NET (c’est-à-dire toute adresse IP).
- $ORACLE_PORTS = n’importe lequel
- $SHELLCODE_PORTS = 180.
- $SIP_PORTS = 5060, 5061, 5600
- $SIP_SERVERS = $HOME_NET (signifie toute adresse IP).
- $SMTP_SERVERS = $HOME_NET (signifie toute adresse IP).
- $SNMP_SERVERS = $HOME_NET (signifie toute adresse IP).
- $SQL_SERVERS = $HOME_NET (c’est-à-dire toute adresse IP).
- $SSH_PORTS = 22.
- $SSH_SERVERS = $HOME_NET (signifie n’importe quelle adresse IP).
- $TELNET_SERVERS = $HOME_NET (c’est-à-dire n’importe quelle adresse IP).

Identifiants du Générateur

L’identifiant de générateur (GID) identifie le sous-système qui évalue une règle de prévention des intrusions et génère des événements. Les règles de prévention des intrusions de texte standard ont un ID de générateur de 1, et les règles de prévention des intrusions d’objets partagés ont un ID de générateur de 3. Il existe également plusieurs ensembles de règles pour divers préprocesseurs. Le tableau suivant explique les GID.

Tableau 1 : ID de générateur

Identifiant	Composant
1	Règle de texte standard

Identifiant	Composant
2	Paquets balisés (Règles pour le générateur de balises, qui génère des paquets à partir d'une session balisée.)
3	Règle des objets partagés
102	Décodeur HTTP
105	Détecteur de Back Orifice
106	Décodeur de RPC
116	Décodeur de paquets
119, 120	Préprocesseur d'inspection HTTP (Les règles GID 120 se rapportent au trafic HTTP spécifique au serveur.)
122	Détecteur de balayage de ports
123	Défragmenteur d'adresses IP
124	Décodeur SMTP (Exploits contre les verbes SMTP.)
125	Décodeur FTP
126	Décodeur Telnet
128	Préprocesseur SSH
129	Préprocesseur de flux
131	Préprocesseur DNS
133	Préprocesseur DCE/RPC
134	Latence des règles, latence des paquets. (Les événements pour ces règles sont générés lorsque la latence des règles suspend (SID 1) ou réactive (SID 2) un groupe de règles d'intrusion, ou lorsque le système cesse d'inspecter un paquet parce que le seuil de latence des paquets est dépassé (SID 3).)
135	Détecteur d'attaque basé sur le débit (Connexions excessives aux hôtes du réseau.)
137	Préprocesseur SSL
138, 139	Préprocesseur de données sensibles
140	Préprocesseur SIP
141	Préprocesseur IMAP

Identifiant	Composant
142	Préprocesseur POP
143	Préprocesseur GTP
144	Préprocesseur Modbus
145	Préprocesseur DNP3

Stratégies d'analyse de réseau

Les politiques d'analyse de réseau contrôlent l'inspection prétraitement du trafic. Les préprocesseurs préparent le trafic à une inspection plus approfondie en le normalisant et en relevant les anomalies de protocole. Le prétraitement lié à l'analyse de réseau a lieu après la mise en correspondance des renseignements de sécurité et le déchiffrement SSL, mais avant le début de l'intrusion ou de l'inspection des fichiers.

Par défaut, le système utilise la politique d'analyse de réseau Sécurité et connectivité équilibrées pour prétraiter tout le trafic géré par une stratégie de contrôle d'accès. Toutefois, si vous configurez une politique de prévention des intrusions sur n'importe quelle règle de contrôle d'accès, le système utilise la politique d'analyse de réseau qui correspond à la politique de prévention des intrusions la plus agressive appliquée. Par exemple, si vous utilisez à la fois des politiques de sécurité sur la connectivité et des politiques équilibrées dans vos règles de contrôle d'accès, le système utilise la Politique d'analyse de réseau (NAP) de sécurité sur la connectivité pour tout le trafic. Pour les politiques de prévention des intrusions personnalisées Snort 3, cette affectation est effectuée conformément à la politique de modèle de base attribuée à la politique de prévention des intrusions.

Lorsque vous utilisez Snort 3, vous pouvez sélectionner une politique explicitement et éventuellement personnaliser ses paramètres. Nous vous recommandons de sélectionner la politique dont le nom correspond à la politique de prévention des intrusions que vous utilisez pour la majeure partie du trafic qui passe par le périphérique, que vous utilisiez la politique de prévention des intrusions directement ou que vous l'utilisiez comme politique de base dans vos politiques de prévention des intrusions personnalisées. Vous pouvez ensuite modifier le mode d'inspection ou ajuster des paramètres d'inspection ou de liaison spécifiques pour prendre en compte le trafic sur votre réseau.

En outre, vérifiez si vous avez activé les règles de préprocesseur dans la politique de prévention des intrusions. Si vous activez des règles qui nécessitent un préprocesseur, activez également l'inspecteur correspondant dans la politique d'analyse de réseau (NAP). Pour chaque inspecteur, vous pouvez également ajuster ses attributs, y compris les ports examinés (binders), afin de personnaliser le comportement de l'inspecteur pour votre réseau.

Remarque Si vous utilisez Snort 2, le système utilise la politique NAP du même nom comme politique de prévention des intrusions la plus restrictive appliquée dans une règle de contrôle d'accès, et vous ne pouvez pas modifier les paramètres des inspecteurs ou des binders.

Exigences de licence pour les politiques de prévention des intrusions

Vous devez disposer de la licence **Menace** pour appliquer des politiques d'intrusion dans les règles d'accès. Pour en savoir plus sur la configuration des licences, consultez Activation ou désactivation des licences facultatives.

Aucune licence supplémentaire n'est nécessaire pour les politiques d'analyse de réseau.

Application des politiques de prévention des intrusions dans les règles de contrôle d'accès

Pour appliquer les politiques de prévention des intrusions au trafic réseau, vous sélectionnez la politique dans une règle de contrôle d'accès qui autorise le trafic. Vous n'attribuez pas directement de politiques de prévention des intrusions.

Vous pouvez attribuer différentes politiques de prévention des intrusions pour fournir une protection contre les intrusions variable en fonction des risques relatifs des réseaux que vous protégez. Par exemple, vous pourriez utiliser la politique de sécurité sur la connectivité, plus stricte, pour le trafic entre votre réseau interne et les réseaux externes. D'un autre côté, vous pouvez appliquer la politique de connectivité sur la sécurité, plus clémente, pour le trafic entre les réseaux internes.

Vous pouvez également simplifier votre configuration en utilisant la même politique pour tous les réseaux. Par exemple, la politique de sécurité et de connectivité équilibrée est conçue pour fournir une bonne protection sans affecter excessivement la connectivité.

Procédure

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

Étape 2 Créez une nouvelle règle ou modifiez une règle existante qui **autorise** le trafic.

En outre, vous pouvez configurer une politique de prévention des intrusions dans le cadre de l'action par défaut si l'action par défaut est allow (autoriser).

Vous ne pouvez pas appliquer de politiques de prévention des intrusions aux règles qui font confiance ou bloquent le trafic.

Étape 3 Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions).

Étape 4 Sélectionnez **Intrusion Policy** > **On** (Politique d'intrusion activée) et sélectionnez la politique d'inspection des intrusions à utiliser pour le trafic correspondant.

Commutation entre Snort 2 et Snort 3

Snort est le moteur d'inspection principal du produit. Bien que vous puissiez changer de version de Snort librement, certaines règles de prévention des intrusions dans Snort 2.0 peuvent ne pas exister dans Snort 3.0, et inversement. Si vous avez modifié l'action d'une règle existante, cette modification n'est pas conservée si vous passez à Snort 3, puis de nouveau à Snort 2, ou de nouveau à Snort 3. Vos modifications apportées aux actions de règles pour les règles qui existent dans les deux versions sont conservées. Notez que le mappage entre les règles dans Snort 3 et Snort 2 peut être un à un ou un à plusieurs, de sorte que la conservation des modifications se fait au mieux.

Si vous modifiez la version de Snort, le système effectuera un déploiement automatique pour mettre en œuvre la modification. Vous pouvez voir la progression dans la Task list (liste des tâches). Les tâches sont Snort Version Change (changement de version Snort) et Automatic Deployment—Snort version toggle (déploiement automatique — basculement de version Snort). En raison du déploiement et du fait que Snort doit être arrêté et redémarré, toutes les connexions existantes, y compris le VPN, sont abandonnées et doivent être rétablies, ce qui entraînera une perte momentanée du trafic.

Remarque Si vous essayez de permuter les versions Snort et que le commutateur échoue, vous aurez des modifications en attente que vous ne pouvez pas ignorer, et une tentative de basculement ultérieure ne sera pas autorisée. Si cela se produit, vous devez effectuer le basculement à l'aide de l'API ToggleInspectionEngine, que vous pouvez utiliser à partir de l'explorateur d'API. Vous devez définir l'attribut bypassPendingChangeValidation à TRUE.

Avant de commencer

Pour déterminer quelle version de Snort est actuellement activée, utilisez cette procédure ou choisissez **Policies (Politiques)** > **Intrusion**. Recherchez la ligne **Snort Version** (Version Snort) au-dessus du tableau. La version actuelle est le premier numéro du numéro de version complet. Par exemple, 2.9.17-95 est une version Snort 2.

Si le périphérique se trouve dans un réseau isolé, considérez le téléversement manuel du dernier ensemble de règles pour la nouvelle version avant le basculement.

Si vous passez à la version 2.0, toutes les politiques de prévention des intrusions personnalisées que vous avez créées sont converties dans les politiques de base utilisées dans la politique personnalisée. Dans la mesure du possible, les remplacements d'actions de règles sont conservés. Si plusieurs politiques personnalisées utilisent la même politique de base, les remplacements de la politique personnalisée utilisée dans la plupart des politiques de contrôle d'accès sont conservés et les remplacements des autres politiques personnalisées sont perdus. Les règles de contrôle d'accès qui utilisaient ces politiques « en double » utiliseront désormais la politique de base créée à partir de votre politique personnalisée la plus utilisée. Toutes les politiques personnalisées sont supprimées. Si vous souhaitez conserver les politiques personnalisées afin de pouvoir les importer ultérieurement, après être passé à Snort 3, utilisez l'API FTD pour exporter la configuration.

En outre, une rétrogradation vers la version 2.0 supprime toutes les personnalisations de politiques d'analyse de réseau (NAP) et le système passe pour utiliser la NAP la plus appropriée en fonction des politiques de prévention des intrusions utilisées dans les règles de contrôle d'accès.

La redirection de nom d'hôte dans l'authentification active nécessite également Snort 3 et sera supprimée si vous passez à Snort 2.

Vous devez déployer toutes les modifications en attente avant de pouvoir changer de version Snort.

Procédure

Étape 1 Sélectionnez **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé des Updates (mises à jour).

Regardez le groupe **Intrusion Rule** (Règles de prévention des intrusions. La version actuelle de Snort est indiquée.

Étape 2 Dans le groupe **Intrusion Rule** (Règles de prévention des intrusions, vous pouvez modifier la version de Snort en cliquant sur **Upgrade to Snort 3.0** (Mise à niveau vers Snort 3.0) ou **Downgrade to Snort 2.0** (Rétrograder à Snort 2.0).

Étape 3 Lorsque vous y êtes invité, sélectionnez l'option d'obtention du dernier ensemble de règles de prévention des intrusions, puis cliquez sur **Yes** (Oui).

Nous vous recommandons d'obtenir le dernier paquet de règles. Le système télécharge les paquets pour la version Snort active uniquement. Il est donc peu probable que le dernier paquet soit installé pour la version Snort vers laquelle vous passez.

Vous devez attendre la fin de la tâche de commutation de versions avant de pouvoir modifier les politiques de prévention des intrusions.

Configuration de Syslog pour les événements d'intrusion

Vous pouvez configurer un serveur syslog externe afin que les politiques de prévention des intrusions envoient des événements d'intrusion à votre serveur syslog. Vous devez configurer le serveur syslog dans la politique de prévention des intrusions pour que les événements d'intrusion soient envoyés au serveur. La configuration d'un serveur syslog sur une règle d'accès envoie uniquement les événements de connexion au serveur syslog, et non les événements d'intrusion.

Si vous sélectionnez plusieurs serveurs syslog, les événements sont envoyés à chacun d'eux.

Les incidents d'intrusion ont l'ID de message 430001.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Intrusion (Prévention des intrusions)**.

Étape 2 Cliquez sur le bouton **Intrusion Policy Settings (Paramètres de la politique d'intrusion)** (⚙) pour configurer syslog.

Étape 3 Cliquez sur le bouton **+** sous **Send Intrusion Events To (envoyer les événements d'intrusion à)** et sélectionnez les objets de serveur qui définissent les serveurs syslog. Si les objets requis n'existent pas déjà, cliquez sur **Create New Syslog Server** (Créer un serveur syslog) et créez-les.

Étape 4 Cliquez sur **OK**.

Configuration de la politique d'analyse de réseau (Snort 3)

La Politique d'analyse de réseau (NAP) est appliquée à toutes les connexions autorisées sur le périphérique. La Politique d'analyse de réseau (NAP) détermine quels inspecteurs sont activés et les valeurs des attributs utilisés par les inspecteurs. Les liens déterminent les ports et les protocoles qui doivent être associés aux différents inspecteurs.

Coordonnez la Politique d'analyse de réseau (NAP) avec les politiques de prévention des intrusions que vous appliquez dans les règles de contrôle d'accès :

- Si vous utilisez une seule politique de prévention des intrusions dans vos règles de contrôle d'accès, sélectionnez la Politique d'analyse de réseau (NAP) du même nom. Apportez ensuite des ajustements aux inspecteurs et aux attributs en fonction des paramètres de votre politique de prévention des intrusions. Par exemple, si vous activez les règles de prévention des intrusions pour un inspecteur en particulier, comme CIP, veillez à activer cet inspecteur dans la Politique d'analyse de réseau (NAP).
- Si vous utilisez plusieurs politiques de prévention des intrusions, sélectionnez la Politique d'analyse de réseau (NAP) qui correspond à la politique de prévention des intrusions la plus stricte que vous utilisez.
- Si vous utilisez des politiques de prévention des intrusions personnalisées, faites votre sélection de Politique d'analyse de réseau (NAP) en fonction de la politique de prévention des intrusions de base pour vos politiques de prévention des intrusions personnalisées.
- Si vous n'avez pas besoin de personnaliser les inspecteurs ou les binders, envisagez de configurer le système afin qu'il sélectionne automatiquement la Politique d'analyse de réseau (NAP) la plus appropriée en fonction de l'utilisation de votre politique de prévention des intrusions. Il s'agit de l'option par défaut.

Avant de commencer

À moins que vous ne l'empêchiez, le système télécharge régulièrement les mises à jour LSP des règles d'inspection. Ces mises à jour peuvent ajouter ou supprimer des inspecteurs et des attributs, et modifier les paramètres par défaut pour les attributs. Si vous avez effectué des remplacements pour des inspecteurs supprimés, ces remplacements sont conservés et vous verrez des avertissements indiquant que l'inspecteur n'est plus pris en charge. Dans ce cas, supprimez l'inspecteur et apportez tous les autres ajustements signalés pour vous assurer que votre Politique d'analyse de réseau (NAP) est entièrement valide.

Procédure

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

Vérifiez que la version de Snort affichée au-dessus du tableau est 3.x.

Étape 2 Cliquez sur le bouton **Intrusion Policy Setting**s (Paramètres de politique de prévention des intrusions) ( ).

Étape 3 Dans **Default Network Analysis Policy** (Politique d'analyse de réseau par défaut), sélectionnez l'une des options suivantes :

- **Auto** : sélectionne automatiquement la Network Analysis Policy (Politique d'analyse de réseau, NAP) correspondant à la politique de prévention des intrusions la plus utilisée (ou à la politique de base pour les règles personnalisées) appliquée dans les règles de contrôle d'accès. Si vous n'appliquez aucune politique d'intrusion, la NAP de sécurité et de connectivité équilibrées est utilisée. La Politique d'analyse

de réseau (NAP) s'exécute en mode Prevention (Prévention), et vous ne pouvez pas personnaliser les paramètres de prévention des intrusions ni les binders. Le reste de cette procédure ne s'applique pas lors de l'exécution en mode automatique.

- **Custom** (Personnalisé) : sélectionne explicitement la NAP qui doit être utilisée. Cliquez sur le lien **Edit** (Modifier) à côté du nom de la politique pour sélectionner une autre politique. Vous pouvez ensuite sélectionner le mode d'inspection et personnaliser les paramètres de l'inspecteur et du classeur selon vos besoins.

Étape 4 Dans la boîte de dialogue Edit (Modifier) Network Analysis Policy (Politique d'analyse de réseau), sélectionnez la politique et configurez ses paramètres.

a) Dans **Network Analysis Policy (Politique d'analyse de réseau)**, sélectionnez la politique qui doit s'appliquer globalement à toutes les connexions autorisées.

b) Choisissez le **Inspection Mode** (Mode d'inspection).

Le mode d'inspection détermine les façons dont le trafic non conforme est géré. Utilisez le même mode d'inspection dans vos politiques de prévention des intrusions pour obtenir des résultats optimaux.

- **Prevention** (Prévention) : bloque toute anomalie de décodeur, de normalisation ou de protocole selon les paramètres définis dans la politique. Vous devez utiliser cette option si vous activez la politique de déchiffrement SSL ou si vous activez l'option **TLS Server Identity Discovery** (Découverte d'identité du serveur TLS) dans les paramètres de la politique de contrôle d'accès.
- **Detection** (Détection) : émet uniquement des alertes en cas d'anomalies de décodeur, de normalisation ou de protocole. Ne bloquez aucun trafic.

c) (Facultatif) Configurez et gérez les remplacements des inspecteurs et des liaisons :

- Pour modifier les remplacements, consultez Configuration des remplacements d'inspector et de binder, à la page 13.
- Pour télécharger le schéma ou les remplacements, consultez Téléchargement des remplacements et du schéma, à la page 15.
- Pour téléverser les remplacements, consultez Chargement des remplacements, à la page 15.
- Pour réinitialiser tous les remplacements, cliquez sur le lien **Reset Inspector/Binder Overrides** (Réinitialiser les remplacements d'inspecteur/liaison) au-dessus du fichier NAP. Vous êtes invité à confirmer l'action. La suppression est limitée aux inspecteurs ou aux classeurs, comme indiqué dans le nom de la commande. Par exemple, la suppression de tous les remplacements de liaison laisse vos remplacements d'inspecteur inchangés.
- Pour annuler toutes les modifications apportées à l'inspecteur sélectionné, cliquez sur **Reset (Réinitialiser)*Inspector (Inspecteur)* aux valeurs par défaut**.
- Pour filtrer l'affichage afin de ne voir que les inspecteurs qui ont des remplacements, cliquez sur **Show Only Overrides** (Afficher uniquement les remplacements). Cliquez sur **Show All Inspectors** (Afficher tous les inspecteurs) pour supprimer le filtre.

d) Cliquez sur **OK**.

Configuration des remplacements d'inspector et de binder

Lorsque vous sélectionnez une Politique d'analyse de réseau (NAP) de base, vous sélectionnez les paramètres d'inspection contenus dans cette politique de base. Dans la plupart des cas, il s'agit des paramètres appropriés.

Cependant, vous pouvez remplacer les paramètres dans la Politique d'analyse de réseau (NAP) sélectionnée. Par exemple, vous pouvez activer ou désactiver des inspecteurs individuels, ou modifier la valeur d'un attribut ou d'un relieur.

La procédure suivante explique comment configurer les remplacements directement. Sinon, vous pouvez télécharger le schéma, apporter des modifications hors ligne, puis charger vos remplacements. Vous pouvez également charger les remplacements que vous avez téléchargés à partir d'un autre périphérique.

Avant de commencer

L'explication de chaque inspecteur, relieur et attribut dépasse la portée de ce document. Pour des informations détaillées, y compris des exemples, consultez *Snort 3 Inspector Reference* (Référence de l'inspecteur Snort 3) à l'adresse https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/snort3-inspectors/snort-3-inspector-reference.html.

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Intrusion**, cliquez sur le bouton **Intrusion Policy Settings (Paramètres de la politique de prévention des intrusions)** ( ), sélectionnez **Custom** (Personnalisé) pour les paramètres de la politique d'analyse de réseau (NAP), puis cliquez sur le lien **Edit** (Modifier) à côté du nom de la politique.

Étape 2 Cliquez sur l'onglet qui contient le paramètre que vous souhaitez modifier :

- **Inspectors** (Inspecteurs) : les inspecteurs examinent des types de trafic précis, comme le FTP, afin de détecter des anomalies de protocole.
- **Binders** : l'inspecteur Binder détermine quand il faut utiliser un inspecteur de service pour inspecter le trafic. Les configurations contenues dans l'inspecteur binder englobent les ports, les hôtes, les CIDR et les services qui déterminent quand un autre inspecteur associé à la même politique d'analyse de réseau doit inspecter le trafic.

Étape 3 Modifiez les paramètres au besoin.

- Utilisez les éléments suivants pour contrôler l'affichage dans l'éditeur JSON :
  - Utilisez la zone d'édition **Filter** (Filtre) pour effectuer une recherche en texte intégral dans le fichier JSON.
  - Cliquez sur le bouton **Expand All Fields** (Développer tous les champs) ( ) pour ouvrir tous les dossiers du fichier JSON.
  - Cliquez sur le bouton **Collapse All Fields** (Réduire tous les champs) ( ) pour fermer tous les dossiers du fichier JSON.
  - Cliquez sur le bouton **Undo Last Action** (Annuler la dernière action) ( ) pour annuler votre modification la plus récente.

- Cliquez sur le bouton **Redo** (Rétablir) ( ) pour rétablir votre dernière modification annulée.
- Sélectionnez **Tree** (Arborescence) pour afficher une vue mise en forme du fichier JSON, qui comprend des menus d'action, des indicateurs d'erreur et d'autres fonctionnalités pour guider vos modifications.
- Sélectionnez **Code** pour afficher le fichier JSON brut.

- Dans la vue Tree (Arborescence), cliquez sur le bouton **Menu** ( ) pour manipuler le contenu du fichier. Vous pouvez réaliser les actions suivantes :
  - **Insert** (Insérer) des attributs. Utilisez Auto pour laisser l'éditeur déterminer le type de données approprié. Sinon, ajoutez Array (Tableau), Object (Objet) ou String (Chaîne). Si vous ajoutez un attribut non valide, le système marquera l'inspecteur ou le lieur comme ayant un problème que vous devez résoudre.
  - **Append** (Ajouter à la fin) des attributs. Cette action fait la même chose que Insert (Insérer), mais place l'attribut à la fin de la section.
  - **Duplicate** (Dupliquer) l'attribut sélectionné.
  - **Remove** (Supprimer) l'attribut sélectionné. Lors de la modification d'un attribut, un message contextuel peut aussi proposer la commande **Delete** (Supprimer).
- Pour activer un inspecteur actuellement désactivé ou modifier le paramètre d'un attribut booléen, cochez la case en regard de la valeur de l'attribut. Par exemple, pour activer un inspecteur, remplacez l'attribut **enabled : false** par :

- Pour modifier la valeur d'un attribut de chaîne ou d'attribut numérique, cliquez dans l'attribut et modifiez la valeur au besoin. Si votre entrée enfreint les règles du champ, des messages d'erreur expliquent l'écart. Par exemple, une valeur numérique indique la plage de valeurs valide si vous saisissez une valeur en dehors de la plage.
- Pour réinitialiser les remplacements :
  - Cliquez sur **Reset Inspector/Binder Overrides** (Réinitialiser les remplacements Inspectors/Binders) pour supprimer toutes vos modifications apportées à tous les inspecteurs ou binders et rétablir les valeurs par défaut. La suppression est limitée aux inspecteurs ou aux lieurs, comme indiqué dans le nom de la commande. Par exemple, la suppression de tous les remplacements de lieurs laissera vos remplacements d'inspecteur inchangés.
  - Cliquez sur **Reset *Inspector* to Defaults** pour annuler toutes les modifications apportées uniquement à l'inspecteur sélectionné.
- Pour filtrer l'affichage afin de ne voir que les inspecteurs qui ont des remplacements, cliquez sur **Show Only Overrides** (Afficher uniquement les remplacements). Cliquez sur **Show All Inspectors** (Afficher tous les inspecteurs) pour supprimer le filtre.
- Si un inspecteur n'est plus pris en charge, il est signalé par un message. Cliquez sur le lien **Delete Inspector** (Supprimer l'inspecteur) dans le message pour supprimer l'inspecteur.

Étape 4 Cliquez sur **OK** lorsque vous avez terminé.

Téléchargement des remplacements et du schéma

Vous pouvez télécharger le schéma NAP ou télécharger les remplacements que vous avez configurés pour la Politique d'analyse de réseau (NAP).

Le téléchargement de remplacements est recommandé chaque fois que vous modifiez la politique d'analyse de réseau (NAP) de base, au cas où vous souhaiteriez revenir à vos paramètres précédents. En outre, vous pouvez utiliser l'éditeur JSON sur un périphérique pour implémenter les remplacements que vous souhaitez utiliser sur tous les périphériques, télécharger les remplacements, puis charger ce fichier de remplacements sur d'autres périphériques.

Le téléchargement du schéma est utile si vous souhaitez modifier le fichier hors ligne, puis charger vos remplacements sur cet appareil ou sur plusieurs périphériques. Vous devez copier et coller uniquement les sections que vous devez modifier, plutôt que de charger le fichier entier, pour vous assurer que seules les modifications que vous apportez sont considérées comme des remplacements.

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Intrusion**, cliquez sur le bouton **Intrusion Policy Settings (Paramètres de la politique de prévention des intrusions)** ( ), sélectionnez **Custom** (Personnalisé) pour les paramètres de la politique d'analyse de réseau (NAP), puis cliquez sur le lien **Edit** (Modifier) à côté du nom de la politique.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour télécharger le schéma de la politique d'analyse de réseau (NAP) actuellement sélectionnée, cliquez sur l'icône en forme d'engrenage ( ) et sélectionnez **Download (Télécharger)** > **Policy Schema (Schéma de politique)**.
- Pour télécharger l'ensemble enregistré de remplacements, tel qu'il existait avant la session de modification actuelle, cliquez sur l'icône en forme d'engrenage ( ) et sélectionnez **Download (Télécharger)** > **Last Saved Overrides (Derniers remplacements enregistrés)**. Le fichier comprend les attributs remplacés et les objets qu'ils contiennent.
- Pour télécharger les remplacements que vous avez créés dans la session de modification actuelle, cliquez sur l'icône en forme d'engrenage ( ) et sélectionnez **Download (Télécharger)** > **Current Unsaved Overrides (Remplacements actuels non enregistrés)**. Le fichier comprend les attributs remplacés et les objets qu'ils contiennent.

Chargement des remplacements

Plutôt que de modifier les attributs à l'aide de l'éditeur JSON intégré, vous pouvez télécharger le schéma de la politique d'analyse de réseau (NAP), modifier le fichier hors ligne, puis téléverser le fichier. Tous les remplacements configurés dans le fichier chargé sont ensuite appliqués à la politique d'analyse de réseau (NAP) sélectionnée.

Vous pouvez également charger un fichier que vous avez téléchargé après avoir configuré des remplacements sur un autre périphérique.

En chargeant vos remplacements, vous pouvez charger le même fichier sur plusieurs périphériques et appliquer facilement les mêmes remplacements.

Avant de commencer

Pour remplacer une configuration d'inspecteur dans la politique d'analyse de réseau, vous devez charger uniquement les modifications dont vous avez besoin. Vous ne devez pas charger la configuration complète, car cela rend les remplacements persistants par nature et, par conséquent, toute modification ultérieure des valeurs ou de la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée. Assurez-vous que les remplacements chargés ciblent précisément les attributs que vous souhaitez modifier.

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Intrusion**, cliquez sur le bouton **Intrusion Policy Settings (Paramètres de la politique de prévention des intrusions)** ( ), sélectionnez **Custom** (Personnalisé) pour les paramètres de la politique d'analyse de réseau (NAP), puis cliquez sur le lien **Edit** (Modifier) à côté du nom de la politique.

Étape 2 Cliquez sur l'icône en forme d'engrenage ( ) et sélectionnez **Upload (Charger)** > **Overrides (Remplacements)**.

Étape 3 (Facultatif) Cliquez sur l'un des liens **Download** (Télécharger) pour enregistrer une copie de vos remplacements existants.

Vous pouvez télécharger les derniers remplacements enregistrés (ceux effectués avant la session de modification actuelle) ou les remplacements non enregistrés actuels (ceux effectués pendant la session de modification actuelle).

Étape 4 Cliquez sur **Yes** (Oui) dans la boîte de dialogue Confirm Upload Overrides (Confirmer le téléversement des remplacements) pour confirmer que vous souhaitez continuer.

Étape 5 Cliquez sur **Browse** (Parcourir), ou faites glisser et déposez pour sélectionner le fichier JSON qui contient vos remplacements, puis cliquez sur **OK**.

Gestion des politiques de prévention des intrusions Snort 3

Lorsque vous utilisez Snort 3 comme moteur d'inspection, vous pouvez créer vos propres politiques de prévention des intrusions et les personnaliser en fonction de vos besoins. Le système est livré avec des politiques prédéfinies qui sont basées sur des politiques définies portant le même nom Cisco Talos Intelligence Group (Talos). Bien que vous puissiez modifier ces politiques, il est préférable de créer votre propre politique à partir de la politique Talos sous-jacente et de modifier celle-ci si vous devez ajuster les actions des règles.

Chacune de ces politiques prédéfinies comprend la même liste de règles de prévention des intrusions (également appelées signatures), mais elles diffèrent par les actions appliquées pour chaque règle. Par exemple, une règle peut être activée dans une politique, mais désactivée dans une autre.

Si vous constatez qu'une règle particulière génère trop de faux positifs, c'est-à-dire qu'elle bloque du trafic que vous ne souhaitez pas bloquer, vous pouvez désactiver la règle sans devoir passer à une politique de

prévention des intrusions moins sécurisée. Vous pouvez également la modifier pour qu'elle génère simplement une alerte lorsqu'il y a correspondance, sans abandonner le trafic.

Inversement, si vous savez que vous devez vous protéger contre une attaque précise, mais que la règle associée est désactivée dans la politique de prévention des intrusions que vous avez choisie, vous pouvez activer la règle sans passer à une politique plus sécurisée.

Utilisez les tableaux de bord liés aux intrusions et le Visualiseur d'événement (tous deux sur la page **Monitoring** (Surveillance)) pour évaluer l'incidence des règles de prévention des intrusions sur le trafic. Gardez à l'esprit que vous ne verrez les incidents d'intrusion et les données de prévention des intrusions que pour le trafic qui correspond aux règles de prévention des intrusions définies sur « alerte » ou « abandon » ; les règles désactivées ne sont pas évaluées.

Remarque Si vous passez à Snort 2, vous ne pouvez pas créer de politiques personnalisées, et l'utilisation des politiques de prévention des intrusions diffère légèrement. Au lieu de cette rubrique, consultez Gestion des politiques de prévention des intrusions (Snort 2), à la page 31.

Procédure

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

Vérifiez que la version de Snort affichée au-dessus du tableau est 3.x.

Étape 2 Effectuez l'une des actions suivantes :

- Utilisez la zone **Search/Filter** (Recherche/filtre) pour trouver une politique. Vous pouvez effectuer une recherche par nom uniquement.
- Cliquez sur l'icône en forme d'engrenage ( ) pour activer la journalisation sur un serveur syslog. Consultez Configuration de Syslog pour les événements d'intrusion, à la page 10.
- Cliquez sur l'icône en forme d'engrenage ( ) pour configurer la politique d'analyse de réseau (Network Analysis Policy, NAP). Consultez Configuration de la politique d'analyse de réseau (Snort 3), à la page 11.
- Cliquez sur + pour créer une nouvelle politique. Consultez Configuration d'une politique de prévention des intrusions personnalisée (Snort 3), à la page 18.
- Cliquez sur l'icône de modification ( ) pour voir les propriétés et les règles de la politique et pour les modifier. Consultez Affichage ou modification des propriétés de la politique de prévention des intrusions (Snort 3), à la page 19.
- Cliquez sur l'icône de suppression ( ) pour supprimer une politique.

Configuration d'une politique de prévention des intrusions personnalisée (Snort 3)

Vous pouvez créer de nouvelles politiques de prévention des intrusions pour personnaliser le comportement des règles si les politiques prédéfinies ne répondent pas à vos besoins. En général, il est conseillé de créer des politiques personnalisées en fonction des politiques prédéfinies plutôt que de modifier ces politiques. Cela vous garantit de pouvoir facilement mettre en œuvre l'une des politiques définies par Cisco Talos si vous trouvez que vos personnalisations ne fournissent pas les résultats dont vous avez besoin.

Procédure

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

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle politique, cliquez sur **+**.
- Pour modifier une règle existante, cliquez sur l'icône de modification ( ) de la règle. Lorsque les détails de la politique sont affichés, cliquez sur le lien **Edit** (Modifier) dans la section des propriétés de la politique en haut de la page.

Étape 3 Saisissez un **nom** et, éventuellement, une description pour cette politique.

Étape 4 Configurez le **mode d'inspection** pour la politique.

- **Prévention**—Les actions découlant d'une règle d'intrusion sont toujours appliquées. Les connexions correspondant à une règle de suppression sont bloquées.
- **Détection** : les règles d'intrusion génèrent uniquement des alertes. Une connexion qui correspond à une règle de suppression génère des messages d'alerte, mais la connexion n'est pas bloquée.

Étape 5 Sélectionnez le **modèle de base** pour la politique.

Les modèles de base sont fournis par Cisco Talos. Cliquez sur l'icône d'information pour chacun pour voir plus d'informations sur les politiques. Notez que les noms de politiques peuvent changer et que de nouvelles politiques peuvent apparaître lorsqu'un nouveau paquet de règles est installé.

- **Détection maximale (Cisco Talos)** : cette politique met l'accent sur la sécurité. La connectivité et le débit du réseau ne sont pas garantis, et des faux positifs sont probables. Cette politique ne doit être utilisée que pour les zones à sécurité élevée, et les moniteurs de sécurité doivent être prêts à enquêter sur les alertes pour déterminer leur validité.
- **Sécurité avant connectivité (Cisco Talos)** : cette politique met l'accent sur la sécurité, au détriment éventuel de la connectivité et du débit du réseau. Le trafic est inspecté plus en profondeur, davantage de règles sont évaluées, et l'on peut s'attendre à des faux positifs et à une augmentation de la latence, mais dans des limites raisonnables.
- **Sécurité et connectivité équilibrées (Cisco Talos)** : (Par défaut.) Cette politique tente de trouver un équilibre subtil entre la connectivité et le débit du réseau, d'une part, et les besoins en matière de sécurité, d'autre part. Bien qu'elle ne soit pas aussi stricte que la politique Sécurité avant connectivité, cette politique vise à assurer la sécurité des utilisateurs tout en étant moins gênante pour le trafic normal.

- **Connectivité avant sécurité (Cisco Talos)** : cette politique met l'accent sur la connectivité et le débit du réseau, au détriment éventuel de la sécurité. Le trafic est inspecté plus superficiellement et moins de règles sont évaluées.
- **Aucune règle active (Cisco Talos)** : il s'agit d'une politique de base qui configure les paramètres de préprocesseur typiques, mais qui n'a aucune règle ni alerte intégrée activée. Utilisez cette politique comme base si vous souhaitez vous assurer que seules les politiques que vous souhaitez appliquer sont activées.

Étape 6 Cliquez sur **OK**.

Vous êtes renvoyé à la liste des politiques de prévention des intrusions. Vous pouvez maintenant afficher la nouvelle politique et ajuster les actions des règles au besoin.

Affichage ou modification des propriétés de la politique de prévention des intrusions (Snort 3)

La page Intrusion Policy (politique de prévention des intrusions) affiche une liste des politiques, y compris les politiques prédéfinies et définies par l'utilisateur, et leurs descriptions. Pour modifier une politique, vous devez d'abord afficher les propriétés de la politique.

Procédure

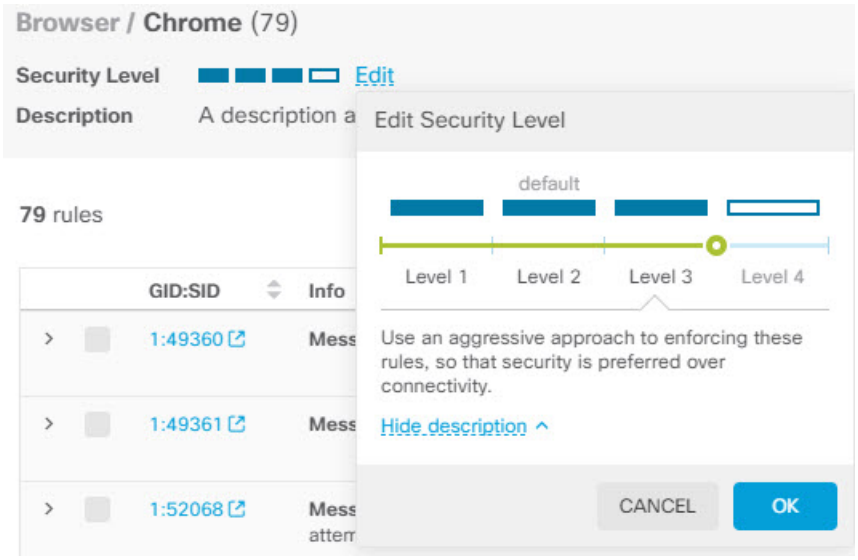
Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

La politique comprend les sections suivantes :

- Liste déroulante **Policy Name (Nom de la politique)**.
  - Vous pouvez facilement passer à une autre politique en la sélectionnant dans la liste déroulante ou revenir à la liste des politiques en cliquant sur le bouton de retour ( ).
  - Vous pouvez supprimer cette politique en cliquant sur l'icône de suppression à côté du nom de la politique ( ).
- **Propriétés générales**. Cette section affiche le mode de prévention des intrusions, la politique de base et la description. Cliquez sur **Edit (Modifier)** pour modifier ces propriétés ou le nom de la politique.
- Table des matières **Rule Group** (Groupe de règles). Cette liste affiche tous les groupes de règles qui ont des règles actives dans la politique. Les groupes ont une hiérarchie, avec des groupes parents contenant des groupes enfants qui organisent des sous-ensembles de règles dans le groupe parent plus grand. Chaque groupe est un ensemble logique de règles, et une règle donnée peut apparaître dans plusieurs groupes.
  - Pour ajouter un groupe qui ne comporte actuellement aucune règle active dans la politique, cliquez sur **+** > **Add Existing Rule Group** (Ajouter un groupe de règles existant) et sélectionnez le groupe. Consultez Ajout ou suppression de groupes de règles dans une politique de prévention des intrusions (Snort 3), à la page 21.

- Pour modifier le niveau de sécurité d'un groupe, sélectionnez le groupe enfant dans la liste. La liste des règles change pour afficher le niveau de sécurité en haut, avec les règles du groupe répertoriées ci-dessous. Cliquez sur le lien **Edit** (Modifier) à côté du niveau de sécurité et sélectionnez un nouveau niveau. Cliquez sur **View Description** (Afficher la description) lors de la modification pour obtenir des renseignements sur chaque niveau de sécurité. Notez que la modification du niveau peut changer les règles actives, ainsi que l'action pour une règle donnée, les niveaux plus sécurisés ayant tendance à avoir davantage de règles actives et plus de règles avec l'action Drop (Abandon). Cliquez sur **OK** pour confirmer la modification. (Le niveau de sécurité ne s'applique pas aux groupes de règles personnalisées.)



- Pour supprimer toutes les règles d'un groupe, sélectionnez le groupe enfant dans la liste. Ensuite, cliquez sur le lien **Exclude** (Exclure) à l'extrémité droite du nom du groupe et confirmez que vous souhaitez exclure le groupe. L'exclusion du groupe désactive simplement toutes les règles du groupe. Cela ne supprime pas le groupe.

  Toutefois, si le groupe comprend des règles partagées avec d'autres groupes activés, les règles partagées conservent toutes les actions appliquées par le groupe toujours actif. Dans tous les cas, nous conservons votre paramètre le plus strict pour une règle individuelle, quelle que soit l'appartenance au groupe.

- Pour ajouter un nouveau groupe de règles personnalisées, cliquez sur **+** > **Upload Custom Rules** (Charger des règles personnalisées) . Pour de plus amples renseignements, consultez la section Téléversement de règles de prévention des intrusions personnalisées, à la page 27.
- Pour modifier le nom ou la description d'un groupe de règles personnalisées, cliquez sur **Edit** (Modifier).
- Pour supprimer un groupe de règles personnalisées, cliquez sur **Delete** (Supprimer). Pour en savoir plus, consultez Gestion des règles de prévention des intrusions personnalisées et des groupes de règles, à la page 25.
- Pour ajouter une nouvelle règle personnalisée dans un groupe de règles personnalisées, cliquez sur le signe + au-dessus du tableau de règles. Consultez Configuration des règles de prévention des intrusions personnalisées individuelles, à la page 29.

- Pour modifier, dupliquer, supprimer ou gérer l'appartenance à un groupe pour une règle personnalisée, passez le curseur sur la droite de la règle et cliquez sur le bouton ou la commande approprié. Pour en savoir plus, consultez Configuration des règles de prévention des intrusions personnalisées individuelles, à la page 29.

- **List of rules** (Liste des règles). Vous pouvez utiliser le champ de recherche pour vous aider à trouver des règles à l'aide de la recherche en texte intégral. Vous pouvez également sélectionner des éléments de filtrage pour effectuer une recherche sur n'importe quelle combinaison de GID ou SID, afficher uniquement les règles définies par l'utilisateur (celles que vous avez ajoutées), ou simplement afficher les règles en fonction de leurs actions : Disabled (désactivée), Alert (alerte) ou Drop (Abandon). Les règles sont chargées au fur et à mesure, de sorte qu'il faut un certain temps pour faire défiler l'ensemble de la liste non filtrée. Lors du filtrage de la liste, cliquez sur le bouton Refresh (Actualiser) pour recharger l'affichage filtré.
  - Pour modifier l'action pour une règle, cliquez sur la case **Action** pour la règle et sélectionnez la nouvelle action, **Alert only** (Alerter uniquement), **Block matching traffic** (Bloquer le trafic correspondant) ou **Disable** (Désactiver). L'action par défaut pour chaque règle est indiquée.
  - Pour modifier l'action pour plus d'une règle à la fois, cochez la case dans la colonne de gauche des règles que vous souhaitez modifier, puis sélectionnez la nouvelle action dans la liste déroulante **Action** au-dessus du tableau des règles. Cochez la case dans l'en-tête GID:SID pour sélectionner toutes les règles de la liste. Vous pouvez modifier jusqu'à 5 000 règles à la fois.
  - Pour mettre à jour les règles dans un groupe de règles personnalisé, cliquez sur **Upload Rule File** (Charger le fichier de règles). Pour en savoir plus, consultez Téléversement de règles de prévention des intrusions personnalisées, à la page 27.
  - Pour obtenir plus d'informations sur une règle, cliquez sur le lien dans la case **GID:SID**. Le lien vous mène vers Snort.org.
  - Pour modifier les règles répertoriées, vous pouvez cliquer sur un groupe enfant dans la table des matières du groupe de règles (et non sur un groupe parent). Vous pouvez revenir à la liste de toutes les règles en cliquant sur **ALL RULES** (TOUTES les règles) en haut de la liste des groupes de règles.
  - Pour modifier l'ordre de tri, cliquez sur l'en-tête de tableau d'une colonne. Le tri par défaut des règles affiche d'abord les règles remplacées, puis celles dont l'action est Drop (abandon), puis celles dont l'action est Alert (alerte).
  - Pour voir les modifications apportées dans une mise à jour de règle de prévention des intrusions (LSP), sélectionnez **LSP Update (Mise à jour LSP)** dans le champ de filtre, puis sélectionnez les mises à jour dont vous souhaitez voir les modifications et précisez si vous souhaitez voir toutes les modifications, ou uniquement les ajouts ou les modifications apportées aux règles.

Ajout ou suppression de groupes de règles dans une politique de prévention des intrusions (Snort 3)

Les règles de prévention des intrusions sont structurées en groupes locaux. Il existe une hiérarchie entre les groupes, avec des groupes parents contenant des groupes enfants associés. Les règles elles-mêmes ne s'affichent

que dans les groupes enfants : les groupes parents sont simplement une structure organisationnelle. Une règle donnée peut apparaître dans plusieurs groupes.

Tous les groupes de règles personnalisées que vous créez se trouvent dans le dossier Groupes définis par l'utilisateur. Les groupes de règles personnalisées n'ont pas de hiérarchie.

La façon la plus simple d'ajouter ou de supprimer des règles dans une politique de prévention des intrusions est d'ajouter ou de supprimer des groupes. Comme les règles d'un groupe sont logiquement liées, il est fort possible que vous souhaitiez utiliser la plupart, si ce n'est toutes les règles d'un groupe donné.

La procédure suivante explique comment ajouter des groupes et modifier le niveau de sécurité du groupe.

Procédure

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

Étape 2 Cliquez sur l'icône Edit (Modifier) ( ) pour le compte que vous souhaitez modifier.

Étape 3 (Ajout de groupes.) Si le groupe ne s'affiche pas dans la liste des groupes de règles, cliquez sur **+** > **Add Existing Rule Group** (Ajouter un groupe de règles existant) et procédez comme suit :

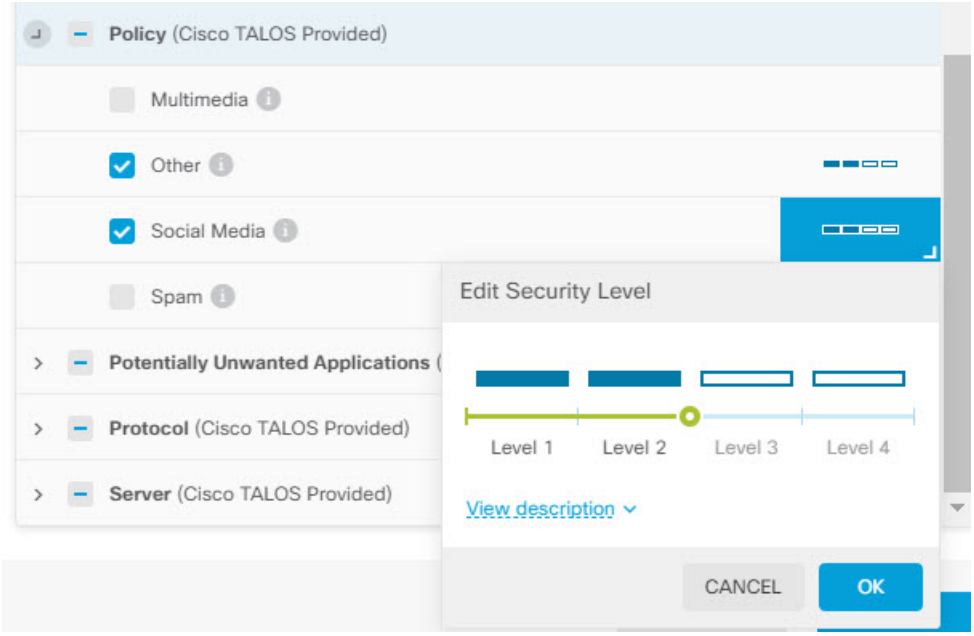
a) Recherchez le groupe enfant.

- Une coche à côté du nom d'un groupe parent indique que tous les groupes enfants du groupe parent sont déjà sélectionnés.
- Un signe moins à côté d'un nom de groupe parent indique qu'un ou plusieurs groupes enfants ne présentent aucune règle activée pour cette politique. Ce sont les groupes que vous pouvez ajouter.
- Une coche à côté d'un nom de groupe enfant indique que le groupe est déjà sélectionné.

b) Sélectionnez le groupe que vous souhaitez ajouter (c'est-à-dire cochez sa case).

c) (Facultatif, ne s'applique pas aux groupes de règles personnalisées.) Chaque groupe a un niveau de sécurité par défaut dépendant de la politique de base utilisée pour la politique personnalisée. Si vous souhaitez le modifier, cliquez sur l'icône du niveau de sécurité, sélectionnez un nouveau niveau, puis cliquez sur **OK**.

Le niveau 1 est la posture la moins sécurisée, car il met l'accent sur la connectivité plutôt que sur la sécurité, tandis que le niveau 4 est la posture la plus stricte et offre une sécurité maximale. Vous pouvez cliquer sur **View Description (Afficher la description)** pour voir une explication de chaque niveau lorsque vous le sélectionnez.



d) Continuez à sélectionner (ou à désélectionner) des groupes jusqu'à ce que vous ayez apporté toutes vos modifications.

e) Cliquez sur **OK**.

Étape 4 (Suppression de groupes.) Si vous souhaitez désactiver toutes les règles dans un groupe, vous pouvez utiliser l'une des méthodes suivantes :

- Sélectionnez le groupe, puis cliquez sur le lien **Exclude** (Exclure) à l'extrémité droite du nom du groupe, au-dessus de la liste des règles.
- Utilisez la méthode pour ajouter un groupe, mais désélectionnez le groupe indésirable (c'est-à-dire décochez sa case) et cliquez sur **OK**.
- Vous pouvez supprimer un groupe de règles personnalisées pour le retirer entièrement du système et de toutes les politiques de prévention des intrusions qui l'utilisent. Sélectionnez le groupe, puis cliquez sur **Delete** (Supprimer).

Modification des actions des règles de prévention des intrusions (Snort 3)

Chaque politique de prévention des intrusions a les mêmes règles. La différence est que l'action entreprise pour chaque règle peut être différente d'une politique à l'autre.

En modifiant l'action découlant d'une règle, vous pouvez désactiver les règles qui vous donnent trop de faux-positifs, ou vous pouvez modifier si la règle alerte ou abandonne le trafic correspondant. Vous pouvez également activer des règles désactivées pour alerter ou abandonner le trafic correspondant.

La méthode la plus simple pour modifier les actions des règles est de modifier le niveau de sécurité d'un groupe de règles. Lorsque vous modifiez le niveau de sécurité d'un groupe, l'action des règles au sein du groupe change. Cela peut signifier que certaines règles sont activées (ou désactivées), ou que l'action peut

changer entre l'alerte et l'abandon, en fonction de l'état de sécurité que vous sélectionnez. Cependant, vous pouvez modifier une action découlant d'une règle individuelle si c'est ce dont vous avez besoin.

Remarque L'action par défaut pour une règle donnée est basée sur la sélection globale du groupe et de la gravité. La modification de la gravité du groupe ou l'exclusion du groupe peut modifier l'action par défaut de la règle.

Avant de commencer

Les groupes de règles personnalisées n'ont pas de niveau de sécurité. Vous ne pouvez pas utiliser la technique du niveau de sécurité pour modifier les actions découlant d'une règle pour des règles personnalisées.

Procédure

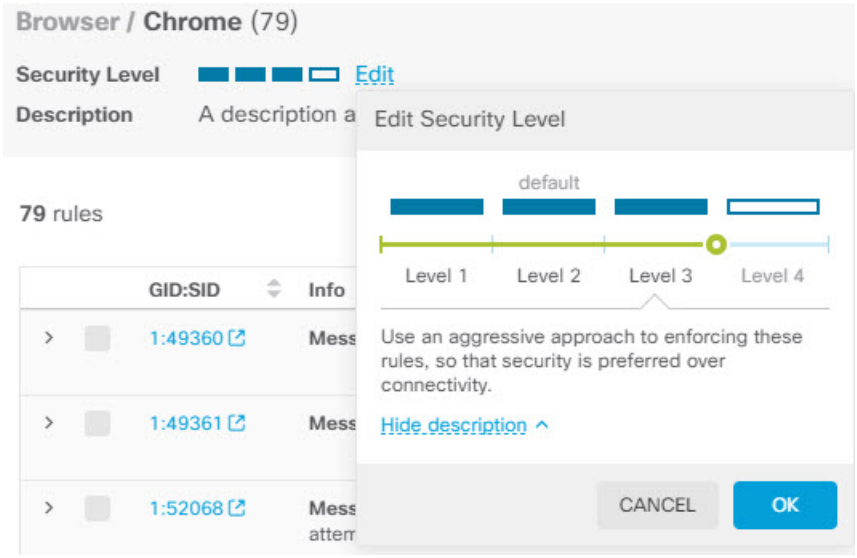
Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur l'icône Afficher ( ) de la politique dont vous souhaitez modifier les actions.

Étape 3 (Méthode recommandée.) Modifier le niveau de sécurité d'un groupe de règles.

a) Cliquez sur le groupe de règles enfant dans la liste des groupes de règles.

b) Au-dessus de la liste des règles, cliquez sur **Edit** (Modifier) à côté du niveau de sécurité du groupe.



Remarque
Si vous souhaitez désactiver toutes les règles du groupe, ne cliquez pas sur **Edit** (Modifier). Au lieu de cela, cliquez sur **Exclude** (Exclure) et confirmez que vous souhaitez exclure le groupe. Le groupe n'est pas supprimé, ses règles sont simplement désactivées. Ignorer les étapes restantes.

c) Sélectionnez le nouveau niveau pour le groupe. Cliquez sur **View Description** (Afficher la description) pour voir une explication de chaque niveau à mesure que vous le sélectionnez.

Le niveau 1 est la posture la moins sécurisée, car il met l'accent sur la connectivité plutôt que la sécurité, tandis que le niveau 4 est la posture la plus dynamique et offre une sécurité maximale.

d) Cliquez sur **OK**.

Étape 4 (Méthode manuelle.) Modifiez l'action pour une ou plusieurs règles.

a) Recherchez la règle dont vous souhaitez modifier l'action.

Utilisez la zone **Search/Filter** (rechercher/filtre) pour rechercher des chaînes dans les informations de règle. Vous pouvez également sélectionner des éléments de filtrage à rechercher sur n'importe quelle combinaison de GID ou SID, ou simplement afficher des règles en fonction de leurs actions (disabled (désactivé), alert (alerte), drop (abandon)). Les règles sont chargées de manière paresseuse, de sorte qu'il faut un certain temps pour faire défiler l'ensemble de la liste non filtrée. Lors du filtrage de la liste, cliquez sur le bouton d'actualisation pour recharger l'affichage filtré.

Idéalement, vous pouvez obtenir l'identifiant Snort (SID) et l'identifiant de Générateur (GID) à partir d'un événement ou auprès de l'assistance technique de Cisco, si vous traitez un problème avec eux. Vous pouvez ensuite rechercher précisément la règle.

b) Pour modifier l'action, procédez comme suit :

- Modifier une règle à la fois : cliquez sur la colonne **Action** pour la règle et sélectionnez l'action requise :
  - **Alert** (Alerte) : crée un événement lorsque cette règle correspond au trafic, mais ne supprime pas la connexion.
  - **Drop** (Abandon) : crée un événement lorsque cette règle correspond au trafic, puis interrompt la connexion.
  - **Disabled** (Désactivé) : ne correspond pas au trafic avec cette règle. Aucun événement n'est généré.
- Modifier plusieurs règles à la fois : cochez les cases des règles que vous souhaitez modifier, puis cliquez sur le menu déroulant **Bulk** au-dessus du tableau et choisissez l'action souhaitée. Cochez la case dans l'en-tête GID:SID pour sélectionner toutes les règles visibles dans la liste. Vous pouvez modifier jusqu'à 5 000 règles à la fois.

Gestion des règles de prévention des intrusions personnalisées et des groupes de règles

Le système est livré avec des règles de prévention des intrusions définies par Cisco Talos Intelligence Group (Talos). Si vous connaissez des attaques supplémentaires, vous pouvez créer et charger des règles de prévention des intrusions personnalisées pour filtrer ces attaques et les alerter ou les supprimer. Vous pouvez également créer, modifier et supprimer une règle à la fois.

Pour les règles chargées, vous créez les règles hors ligne à l'aide d'un éditeur de texte. Nous vous recommandons d'inclure un groupe de règles personnalisées dans chaque fichier texte que vous chargez. Vous pouvez ensuite facilement charger les modifications de vos règles et soit fusionner les nouvelles règles dans vos groupes de règles personnalisés, soit remplacer vos règles par des copies nouvelles et modifiées.

L'explication de la création de ces règles n'entre pas dans le cadre de ce document. Pour des informations détaillées sur la façon d'écrire des règles de prévention des intrusions pour Snort, y compris la conversion des règles Snort 2 au format Snort 3, consultez les guides sur https://snort.org/documents. Par exemple, *Règles*

d'introduction à l'écriture de règles Snort 3 à l'adresse https://snort.org/documents/rules-writers-guide-to-snort-3-rules.

Avant de commencer

Vous créez des groupes de règles personnalisés pendant le processus de chargement des règles personnalisées, comme décrit dans Téléversement de règles de prévention des intrusions personnalisées, à la page 27, ou lors de la création de règles individuelles ou de la gestion de l'appartenance des règles. Après avoir créé le groupe, vous pouvez gérer le groupe et son contenu.

Notez que les groupes personnalisés sont disponibles pour toutes les politiques de prévention des intrusions, pas seulement pour la politique que vous modifiez lors de la création du groupe. Ainsi, les modifications que vous apportez à un groupe sont appliquées à toutes les politiques. Par exemple, si vous supprimez un groupe de règles personnalisées, il est supprimé de toutes les politiques et n'est plus disponible pour aucune d'entre elles.

Procédure

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

Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

Nous vous recommandons d'ajouter des règles personnalisées à une politique de prévention des intrusions personnalisée plutôt que l'une des politiques intégrées.

Étape 3 Effectuez l'une des actions suivantes :

- Pour créer un groupe, cliquez sur le signe plus **(+)** > **Upload Custom Rules** (Charger des règles personnalisées) . Consultez Téléversement de règles de prévention des intrusions personnalisées, à la page 27.
- Pour modifier le nom ou la description d'un groupe, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Vous pouvez ensuite cliquer sur **Edit** (Modifier) et apporter vos modifications.
- Pour exclure le groupe et ses règles de la politique, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Vous pouvez ensuite cliquer sur **Exclude** (Exclure) pour supprimer le groupe.
- Pour supprimer le groupe du système et toutes les politiques qui l'utilisent, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Cliquez sur **Delete** (Supprimer). Notez que si une règle n'existe que dans le groupe supprimé, elle est également supprimée du système. Toutefois, si une règle existe également dans d'autres groupes de règles personnalisées que vous ne supprimez pas, la règle reste dans ces groupes.
- Pour remplacer ou mettre à jour les règles d'un groupe en bloc, sélectionnez le groupe dans la table des matières du groupe dans le dossier Groupes définis par l'utilisateur. Ensuite, cliquez sur **Upload Rule File** (Charger le fichier de règles) à côté de la liste déroulante Action au-dessus du tableau de règles du groupe. Le processus est le même que celui décrit dans Téléversement de règles de prévention des intrusions personnalisées, à la page 27.

- Pour créer et gérer des règles individuelles et leur affectation à des groupes de règles, consultez Configuration des règles de prévention des intrusions personnalisées individuelles, à la page 29.

Téléversement de règles de prévention des intrusions personnalisées

Si vous connaissez des attaques qui ne sont actuellement pas couvertes par d'autres règles, vous pouvez créer et téléverser des règles de prévention des intrusions personnalisées pour filtrer ces attaques et générer une alerte ou abandonner le trafic. L'action des règles importées doit être « alert (alerte) » ou « drop (abandon) », et l'action par défaut de la règle est définie par l'action indiquée dans le fichier importé. Une fois importées, vous pouvez modifier l'action d'une règle et désactiver une règle au besoin.

Vous devez créer ces règles hors ligne. Dans cet écran FDM, vous chargez simplement un fichier de règles ; vous ne configurez pas les règles directement. Le fichier de règles doit être un fichier texte. Vous pouvez utiliser des retours de ligne pour formater les règles afin qu'elles soient lisibles, ou placer une règle sur une seule ligne ; les lignes vides sont autorisées. Le format des règles est expliqué sur snort.org.

Par exemple, un fichier de téléversement de trois règles peut ressembler à ce qui suit :

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
   gid:1;
   sid:1000002;
```

```
    rev:1;
)
```

Procédure

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

Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

Nous vous recommandons d'ajouter des règles personnalisées à une politique de prévention des intrusions personnalisée plutôt qu'à l'une des politiques intégrées.

Étape 3 Effectuez l'une des opérations suivantes :

- Au-dessus de la liste des groupes, cliquez sur **+** > **Upload Custom Rules** (Charger des règles personnalisées) .
- Si vous téléversez des règles dans un groupe de règles personnalisées que vous avez déjà créé, vous pouvez sélectionner le groupe de règles personnalisées, puis cliquer sur **Upload Rule File** (Charger le fichier de règles) à côté de la liste déroulante **Action** au-dessus du tableau de règles du groupe.

Étape 4 Cliquez sur **Browse** (Parcourir) et sélectionnez votre fichier de règle personnalisé, ou faites glisser le fichier et déposez-le dans la boîte de dialogue Upload File (Charger le fichier).

Attendez que le chargement soit terminé.

Étape 5 Sélectionnez la façon dont vous souhaitez gérer les conflits :

Il y a conflit lorsqu'une règle que vous ajoutez est identique à une règle déjà présente dans le système. Cela devrait se produire uniquement si vous téléversez les mêmes règles ou des versions modifiées de règles que vous avez déjà chargées.

Sélectionnez une des options :

Remarque
Les options **Merge** (Fusionner) et **Replace** (Remplacer) sont essentiellement la même chose. Les règles chargées doivent avoir des numéros de révision plus élevés que celles que vous avez déjà téléversées pour que des modifications soient apportées aux règles existantes. La seule différence est que si le fichier de chargement ne contient pas certaines règles présentes dans le groupe de règles personnalisées ciblé, l'option **Replace** (Remplacer) supprimera ces règles du groupe de règles. L'option **Merge** (Fusionner) laissera ces règles « manquantes » en place.

- **Merge** (Fusionner) : pour toute règle modifiée dans le fichier téléversé qui existe également dans le groupe sélectionné, ces modifications seront fusionnées si la règle dans le fichier téléversé a un numéro de révision plus élevé. Toutes les règles inchangées, ou les règles du groupe qui n'ont pas de règles correspondantes dans le téléversement, resteront inchangées. Toutes les nouvelles règles dans le chargement seront ajoutées. Il s'agit de l'option par défaut.
- **Replace** (Remplacer) : les règles dans le fichier chargé remplaceront les règles du groupe sélectionné si le numéro de révision de la règle chargée est supérieur. Toutes les règles existantes qui ne figurent pas dans le fichier chargé seront supprimées du groupe. Les règles existantes dont la version chargée a un numéro de révision identique ou inférieur resteront inchangées. Toutes les nouvelles règles dans le chargement seront ajoutées.

Étape 6 Cliquez sur + et sélectionnez le groupe de règles personnalisées pour les règles chargées.

Si le groupe de règles personnalisées que vous souhaitez utiliser n'existe pas encore, cliquez sur **Create New Group** (Créer un nouveau groupe) et créez-le maintenant. Le nouveau groupe a besoin d'un nom et, éventuellement, d'une description. Vous pouvez ensuite sélectionner le nouveau groupe.

Si vous remplacez des règles, vous ne pouvez sélectionner qu'un seul groupe. Si vous les fusionnez, vous pouvez sélectionner plusieurs groupes.

Étape 7 Cliquez sur **OK**.

Les fichiers sont chargés et placés dans le nouveau groupe. Vous devriez voir un résumé du nombre de règles qui ont été chargées et du nombre de règles mises à jour, supprimées ou ignorées.

S'il y a des erreurs dans le fichier, le chargement échouera. Vous pouvez cliquer sur le lien **Download Error File** (Télécharger le fichier d'erreurs) pour obtenir plus d'informations sur les erreurs.

Le groupe est automatiquement activé dans cette politique de prévention des intrusions. Le groupe et les nouvelles règles peuvent être ajoutés à d'autres politiques, mais le groupe et les règles ne sont automatiquement activés dans aucune autre politique. Pour en savoir plus sur l'ajout de groupes à d'autres politiques, consultez Ajout ou suppression de groupes de règles dans une politique de prévention des intrusions (Snort 3), à la page 21.

Configuration des règles de prévention des intrusions personnalisées individuelles

Vous pouvez configurer des règles de prévention des intrusions personnalisées une à la fois plutôt qu'en bloc par le biais du téléversement de fichiers. Cette méthode fonctionne bien lorsque vous devez effectuer un ajustement rapide à une règle ou que vous ne devez créer ou modifier que quelques règles à la fois.

Lors de la configuration des règles de prévention des intrusions, gardez les éléments suivants à l'esprit :

- Le GID de toutes les règles personnalisées doit être 1.
- Le SID d'une règle doit être unique pour toutes les règles du système. Il doit également être d'un million (1 000 000) ou plus.
- Si vous modifiez une règle, vous devez changer la version de la règle. Normalement, vous incrémentez le numéro de version de 1.
- Vous pouvez dupliquer une règle Cisco Talos Intelligence Group (Talos) pour créer votre propre version de la règle, mais vous devez toujours modifier le SID du doublon pour le rendre unique.

Le système effectuera des vérifications de validité pour s'assurer que la règle est bien formée, et vous verrez des messages d'erreur pour tout problème. Cependant, le système ne peut pas déterminer si la règle est sensible.

Pour des informations détaillées sur la façon d'écrire des règles de prévention des intrusions pour Snort, y compris la conversion des règles Snort 2 au format Snort 3, consultez les guides sur https://snort.org/documents. Par exemple, *Règles d'introduction à l'écriture de règles Snort 3* à l'adresse https://snort.org/documents/rules-writers-guide-to-snort-3-rules.

Procédure

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

Étape 2 Cliquez sur l'icône de modification ( ) d'une politique.

Nous vous recommandons d'ajouter des règles personnalisées à une politique de prévention des intrusions personnalisée plutôt qu'à l'une des politiques intégrées.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour ajouter une règle de prévention des intrusions, cliquez sur le bouton **Add New Intrusion Rule** (Ajouter une nouvelle règle de prévention des intrusions) (+) au-dessus du tableau de règles. Lors de l'ajout d'une règle, vous devez sélectionner un ou plusieurs groupes de règles personnalisés pour contenir la nouvelle règle. Vous pouvez créer de nouveaux groupes tout en ajoutant la règle, au besoin.
- Pour ajouter une règle en dupliquant et en modifiant une règle existante, passez le curseur à l'extrémité droite de la règle, puis cliquez sur le bouton Duplicate (Dupliquer) ( ). Le bouton s'affiche uniquement lorsque vous passez le curseur. Pour les règles personnalisées, la commande **Duplicate** (Dupliquer) se trouve sous le bouton More Options (Plus d'options) (**...**).
- Pour modifier une règle personnalisée, recherchez la règle dans un groupe de règles personnalisées et cliquez sur le bouton de modification ( ) pour la règle. Vos modifications s'appliquent à tous les groupes dans lesquels la règle se trouve. Assurez-vous d'incrémenter le numéro de version de la règle d'au moins 1 lorsque vous apportez des modifications.
- Pour supprimer une règle personnalisée, cliquez sur le bouton de suppression ( ) correspondant à la règle. La règle est supprimée de tous les groupes de règles qui la contiennent. Si vous souhaitez simplement supprimer une règle d'un groupe, utilisez l'option **Manage Group Assignments** (Gérer les affectations de groupe) au lieu de supprimer la règle.
- Pour modifier les groupes qui contiennent la règle, cliquez sur le bouton More Options (Plus d'options) (**...**) et sélectionnez **Manage Group Assignments** (Gérer les affectations de groupe). Vous pouvez ensuite ajouter ou supprimer des groupes. Vos modifications affectent simplement l'appartenance au groupe, elles ne modifient pas la règle et ne la suppriment pas.

Étape 4 Pour les nouvelles règles et les groupes, ajoutez la règle à la politique.

Lorsque vous créez un nouveau groupe lors de la création d'une nouvelle règle ou de la modification d'une règle existante, ce groupe n'est pas ajouté automatiquement à votre politique et la règle n'est pas activée automatiquement. Vous êtes invité à ajouter le groupe à la politique que vous modifiez. Si vous n'ajoutez pas le groupe lors de l'ajout ou de la modification de la règle, vous pouvez ajouter le groupe ultérieurement en utilisant le processus suivant :

a) Cliquez sur **+** > **Add Existing Rule Group** > **(Ajouter un groupe de règles existant)** au-dessus de la table des matières du groupe.
b) Recherchez le groupe dans le dossier User Defined Groups (Groupes définis par l'utilisateur), sélectionnez-le, puis cliquez sur **OK**.
c) Sélectionnez le groupe dans la table des matières et vérifiez que la nouvelle règle se trouve dans le groupe et comporte l'action souhaitée.

Gestion des politiques de prévention des intrusions (Snort 2)

Vous pouvez appliquer n'importe quelle politique de prévention des intrusions prédéfinie. Chacune de ces politiques comprend la même liste de règles de prévention des intrusions (également appelées signatures), mais elles varient dans les actions prises pour chaque règle. Par exemple, une règle peut être active dans une politique, mais désactivée dans une autre politique.

Si vous trouvez qu'une règle particulière vous donne trop de faux positifs, où la règle bloque le trafic que vous ne souhaitez pas bloquer, vous pouvez désactiver la règle sans avoir à passer à une politique de prévention des intrusions moins sécurisée. Vous pouvez également le modifier pour qu'il soit signalé par une alerte pour les correspondances sans perte du trafic.

Inversement, si vous savez que vous devez vous protéger contre une attaque spécifique, mais que la règle associée est désactivée dans la politique de prévention des intrusions de votre choix, vous pouvez activer la règle sans passer pour une politique plus sécurisée.

Utilisez les tableaux de bord liés aux intrusions et le Visualiseur d'événement (tous deux sur la page **Monitoring** (Surveillance)) pour évaluer l'incidence des règles de prévention des intrusions sur le trafic. Gardez à l'esprit que vous ne verrez les incidents d'intrusion et les données de prévention des intrusions que pour le trafic qui correspond aux règles de prévention des intrusions définies sur « alerte » ou « abandon »; les règles désactivées ne sont pas évaluées.

Les rubriques suivantes expliquent plus en détail les politiques de prévention des intrusions et le réglage des règles.

Configurer le mode d'inspection d'une politique de prévention des intrusions (Snort 2)

Par défaut, toutes les politiques de prévention des intrusions fonctionnent en mode de prévention pour mettre en œuvre un système de prévention des intrusions (IPS). En mode d'inspection de prévention, si une connexion correspond à une règle de prévention des intrusions dont l'action est d'abandonner le trafic, la connexion est activement bloquée.

Si vous souhaitez plutôt tester l'effet de la politique de prévention des intrusions sur votre réseau, vous pouvez passer au mode de détection, qui implémente un système de détection des intrusions (IDS). Dans ce mode d'inspection, les règles de rejet sont traitées comme des règles d'alerte, où vous êtes informé des connexions correspondantes, mais le résultat de l'action devient « aurait bloqué », et les connexions ne sont jamais bloquées.

Vous modifiez le mode d'inspection par politique de prévention des intrusions, de sorte que vous pouvez avoir une combinaison de prévention et de détection.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Intrusion (Prévention des intrusions)**.

Étape 2 Cliquez sur l'onglet de la politique de prévention des intrusions dont vous souhaitez modifier le mode d'inspection.

Le **Inspection Mode** (Mode d'inspection) est indiqué au-dessus du tableau de règles.

Étape 3 Cliquez sur le lien **Edit (Modifier)** à côté du mode d'inspection, modifiez le mode pour la politique, puis cliquez sur **OK**.

Les options sont les suivantes :

- **Prevention** (Prévention) : les actions découlant d'une règle d'intrusion sont toujours appliquées. Les connexions correspondant à une règle de suppression sont bloquées.
- **Detection** (Détection) : les règles d'intrusion génèrent uniquement des alertes. Une connexion qui correspond à une règle de suppression génère des messages d'alerte, mais la connexion n'est pas bloquée.

Modification des actions des règles de prévention des intrusions (Snort 2)

Chaque politique de prévention des intrusions prédéfinie comporte les mêmes règles. La différence est que l'action entreprise pour chaque règle peut être différente d'une politique à l'autre.

En modifiant l'action découlant d'une règle, vous pouvez désactiver les règles qui vous donnent trop de faux-positifs, ou vous pouvez modifier si la règle alerte ou abandonne le trafic correspondant. Vous pouvez également activer des règles désactivées pour alerter ou abandonner le trafic correspondant.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Intrusion (Prévention des intrusions)**.

Étape 2 Cliquez sur l'onglet de la politique de prévention des intrusions dont vous souhaitez modifier les actions de règle.

Les politiques prédéfinies sont les suivantes :

- Connectivité avant la sécurité
- Sécurité et connectivité équilibrées
- Sécurité avant la connectivité
- Détection maximale

Étape 3 Recherchez la règle dont vous souhaitez modifier l'action.

Les règles sont triées en affichant d'abord celles qui ont été remplacées, puis par action au sein du groupe des règles remplacées. Sinon, les règles sont triées par GID, puis par SID.

Utilisez la zone de recherche pour localiser la règle que vous souhaitez modifier. Idéalement, vous pouvez obtenir l'identifiant Snort (SID) et l'identifiant de Générateur (GID) à partir d'un événement ou auprès de l'assistance technique de Cisco, si vous traitez un problème avec eux.

Pour des informations détaillées sur les éléments de chaque règle, consultez Attributs des règles d'intrusion, à la page 3.

Pour effectuer une recherche dans la liste :

a) Cliquez dans la zone **Search** (Rechercher) pour ouvrir la boîte de dialogue des attributs de recherche.

b) Saisissez une combinaison d'ID de Générateur (**GID**), d'ID Snort (**SID**) ou **d'action** de règle, puis cliquez sur **Search** (Rechercher).

Par exemple, vous pourriez sélectionner **Action = Drop** pour voir toutes les règles de la politique qui bloqueront les connexions correspondantes. Le texte à côté de la zone de recherche indique le nombre de règles correspondant à vos critères, par exemple, « 8937 sur 9416 règles trouvées ».

Pour effacer un critère de recherche, cliquez sur le x pour le critère dans la zone de recherche.

Étape 4 Cliquez sur la colonne **Action** pour la règle et sélectionnez l'action requise :

- **Alert** (Alerte) : crée un événement lorsque cette règle correspond au trafic, mais ne supprime pas la connexion.
- **Drop** (Abandon) : crée un événement lorsque cette règle correspond au trafic, puis interrompt la connexion.
- **Disabled** (Désactivé) : ne correspond pas au trafic avec cette règle. Aucun événement n'est généré.

L'action par défaut de la règle est indiquée par « (Default) » ajouté à l'action. Si vous modifiez la valeur par défaut, la colonne d'état indique « Overridden » (Remplacer) pour cette règle.

Surveillance des politiques de prévention des intrusions

Vous pouvez trouver les statistiques de politique de prévention des intrusions dans les tableaux de bord **Attackers** (attaquants) et **Targets** (cibles) sur la page **Monitoring** (surveillance). 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. Consultez Tableaux de bord du trafic et du système.

Pour voir les incidents d'intrusion, sélectionnez **Monitoring (Surveillance)** > **Events (Événements**, puis cliquez sur l'onglet **Intrusion**. Vous pouvez placer le curseur sur un événement et cliquer sur le lien **View Details** (afficher les détails) pour obtenir plus d'informations. Dans la page des détails, vous pouvez cliquer sur **View IPS Rule** (afficher la règle IPS) pour accéder à la règle dans la politique de prévention des intrusions appropriée, où vous pouvez modifier l'action associée à la règle. Cela peut vous aider à réduire l'impact des faux positifs, lorsqu'une règle bloque trop de bonnes connexions, en modifiant l'action de drop (abandon) à alert (alerte). Inversement, vous pouvez transformer une règle d'alerte (alert rule) en règle de rejet (drop rule) si vous voyez beaucoup de trafic d'attaque pour une règle.

Si vous configurez un serveur syslog pour la politique de prévention des intrusions, les incidents d'intrusion ont l'ID de message 430001.

Exemples de politiques de prévention des intrusions

Le chapitre sur les intrusions comprend les exemples suivants de mise en œuvre des politiques de prévention des intrusions.

- Comment bloquer les menaces
- Comment surveiller passivement le trafic sur un réseau

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.