



Stratégies de prévention des intrusions

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.

- [Politique de prévention des intrusions](#) , à la page 1
- [Création d'une politique de prévention des intrusions Snort 3 personnalisée](#), à la page 3
- [Modification des politiques de prévention des intrusions Snort 3](#), à la page 4
- [Modifier la politique de base d'une politique de prévention des intrusions](#), à la page 10
- [Afficher le mappage de politique de base Snort 2 et Snort 3](#), à la page 10
- [Synchroniser les règles de Snort 2 avec celles de Snort 3](#), à la page 11
- [Gérer les politiques de prévention des intrusions](#), à la page 13
- [Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions](#), à la page 14
- [Régler les politiques de prévention des intrusions à l'aide de règles](#), à la page 16
- [Règles recommandées](#), à la page 37
- [Atténuer les menaces à l'aide du cadre MITRE dans les politiques de prévention des intrusions Snort 3](#), à la page 42

Politique de prévention des intrusions

Une *politique de prévention des intrusions* est un ensemble défini de configurations de détection et de prévention des intrusions qui

- inspecte le trafic pour détecter les violations de sécurité,
- peut bloquer ou modifier le trafic malveillant dans les déploiements en ligne, et
- sert de dernière ligne de défense du système avant que le trafic ne soit autorisé à se rendre à 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 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 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.

Par défaut, le système désactive l'inspection des charges utiles chiffrées. Cette valeur par défaut réduit les faux positifs et améliore les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès avec l'inspection de prévention des intrusions activée.

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](#).

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

Créez une politique de prévention des intrusions Snort 3 personnalisée pour adapter les paramètres de détection et de prévention des intrusions aux exigences de sécurité de votre réseau.

Les politiques de prévention des intrusions Snort 3 définissent la façon dont le système inspecte le trafic et répond aux menaces potentielles. Vous pouvez créer des politiques personnalisées en fonction des politiques existantes fournies par le système ou d'autres politiques personnalisées pour répondre à des besoins de sécurité spécifiques.

Before you begin

Suivez les étapes suivantes pour créer une politique de prévention des intrusions Snort 3 personnalisée :

Procédure

Étape 1 Choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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

Utilisez cette tâche pour comprendre comment accéder, modifier et gérer les politiques de prévention des intrusions Snort 3 dans le centre de gestion de pare-feu, y compris la modification des paramètres de politique, la gestion des groupes de règles et l'application de recommandations pour protéger votre réseau.

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

Before you begin

-

Procédure

- Étape 1** Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.
- Étape 3** Cliquez sur **Version Snort 3** à côté de la politique de prévention des intrusions que vous souhaitez configurer.
- Étape 4** Modifier votre politique
 - Change the mode (modifier le mode) : Cliquez sur le menu déroulant **Mode** pour modifier le mode d'inspection.



Mise en garde

Le mode d'inspection est modifié uniquement pour la version Snort 3 de la politique. Le mode d'inspection existant est conservé dans la version Snort 2 tel quel, ce qui signifie que vos versions Snort 2 et Snort 3 de la politique auront des modes d'inspection différents. Nous vous recommandons d'utiliser cette option avec prudence.

- **Prevention** (Prévention) : les règles de blocage déclenchées créent un événement (alerte) et abandonnent la connexion.
- **Detection** (Détection) : les règles de blocage déclenchées créent une alerte.

Vous pouvez choisir le mode de détection avant de choisir la prévention. Par exemple, avant de choisir le mode de prévention, vous pouvez souhaiter que les règles de blocage envoient uniquement des alertes, afin de vous permettre d'identifier les règles qui provoquent de nombreux faux positifs.

- Étape 5** Cliquez sur la couche **Politique de base** qui définit les paramètres par défaut de la politique de prévention des intrusions.
 - Search Rules (règles de recherche) : utilisez le champ de recherche pour filtrer l'affichage. Vous pouvez saisir le GID, la SID, le message de règle ou des informations de référence. Par exemple, GID:1; SID:9621 (pour afficher uniquement la règle 1:962, SID :9621,9622,9623) pour afficher plusieurs règles avec différents SID. Vous pouvez également cliquer dans la zone de texte Rechercher pour choisir l'une des options suivantes :
 - appliquez les filtres **Action = Alerte** ou **Actio : Block (Blocage)**.

- appliquer le filtre **Règles désactivées**
- afficher **les règles personnalisées/définies par l'utilisateur**
- filtrer par GID, SID ou GID:SIDf
- filtrer par CVE
- filtrer par commentaire
- View filtered Rules (afficher les règles filtrées) : cliquez sur l'un des paramètres **prédéfinis** pour afficher les règles qui sont définies pour alerter, bloquer, désactiver, etc.

Les règles remplacées indiquent les règles dans lesquelles l'action de règle a été remplacée par une action différente de l'action par défaut. Notez qu'une fois modifié, l'état de l'action découlant de la règle est Overridden même si vous lui rétablissez son action par défaut d'origine. Cependant, si vous sélectionnez **Revert to Default** (Revenir aux valeurs par défaut) dans la liste déroulante **Rule Action** (Actions de règles), l'état Overridden (Remplacé) est supprimé.

Les filtres avancés fournissent des options de filtre en fonction des versions du paquet de sécurité allégé (LSP), des classifications des intrusions et des vulnérabilités Microsoft.

- Afficher la documentation de la règle : cliquez sur l'ID de règle ou sur l'icône **Rule Documentation** (documentation de la règle) pour afficher la documentation Talos sur la règle.
- Afficher les détails d'une règle : cliquez sur l'icône **Flèche Développer** (➤) dans une ligne de règle pour afficher les détails de la règle.
- Ajouter des commentaires sur une règle : cliquez sur **Commentaires** (📝) dans la colonne Commentaires pour ajouter des commentaires concernant une règle.

Étape 6

Group Overrides (Remplacement de groupes) : cliquez sur la couche **Group Overrides** (Remplacement de groupes) qui répertorie toutes les catégories de groupes de règles. Le groupe de règles parent de niveau supérieur avec la description, les remplacements, les groupes activés et d'autres détails s'affiche. Les groupes de règles parents ne peuvent pas être mis à jour et sont en lecture seule. Seuls les groupes de règles feuille peuvent être mis à jour. Dans chaque groupe de règles, vous pouvez traverser jusqu'au dernier groupe feuille. Dans chaque groupe, vous pouvez remplacer, inclure et exclure des groupes de règles. Dans les groupes de règles feuille, vous pouvez :

- Search Rule Groups (rechercher des groupes de règles) : utilisez le champ de recherche pour saisir des mots-clés et rechercher des groupes de règles.
- Dans le panneau de gauche, vous pouvez choisir l'une des options de filtre prédéfinies pour rechercher des groupes de règles :
 - All (tout) : pour afficher tous les groupes de règles.
 - Excluded (Exclus) : pour les groupes exclus.
 - Included (Inclus) : pour les groupes inclus.
 - Overridden (Remplacé) : pour la configuration de groupe de règles qui est remplacée.
- Définir le niveau de sécurité d'un groupe de règles : accédez au groupe de règles requis dans le volet de gauche et cliquez dessus. Cliquez sur **Modifier** à côté du **niveau de sécurité** du groupe de règles pour augmenter ou diminuer le niveau de sécurité en fonction des paramètres de règle définis par le système.

Dans la boîte de dialogue **Edit Security Level** (Modifier le niveau de sécurité), vous avez la possibilité de cliquer sur **Revert to Default** (Revenir au niveau par défaut) pour rétablir les modifications que vous avez effectuées.

Firewall Management Center modifie automatiquement l'action pour les règles du groupe de règles en fonction du niveau de sécurité configuré. Dans la couche **Rule Overrides** (Remplacements de règles), notez le nombre de règles Block (blocage) et de règles Disabled (désactivées) dans les **présélections** chaque fois que vous modifiez le niveau de sécurité.

- Vous pouvez apporter des modifications en bloc au niveau de sécurité pour modifier le niveau de sécurité de tous les groupes de règles d'une catégorie de règles particulière. Le niveau de sécurité en bloc s'applique aux groupes de règles qui ont plusieurs groupes de règles. Après une mise à jour en bloc de groupes de règles, vous pouvez toujours mettre à jour le niveau de sécurité de n'importe quel groupe de règles qui y est associé.

Il peut y avoir des niveaux de sécurité **mixtes** au sein des groupes de règles; **mixte** indique que les groupes enfants contiennent un mélange de niveaux de sécurité au sein du groupe de règles parent.

- Inclure ou exclure des groupes de règles : les groupes de règles affichés sont les groupes de règles par défaut associés à la politique de base de prévention des intrusions fournie par le système. Vous pouvez inclure et exclure des groupes de règles de la politique de prévention des intrusions. Un groupe de règles exclu est supprimé de la politique de prévention des intrusions et ses règles ne sont pas appliquées au trafic. Pour en savoir plus sur le chargement de règles personnalisées dans Firewall Management Center, consultez [Ajouter des règles personnalisées aux groupes de règles, à la page 32](#).

Pour exclure un groupe de règles :

1. Naviguez dans le volet Rule Groups (Groupes de règles) et choisissez le groupe de règles que vous souhaitez exclure.
2. Cliquez sur le lien hypertexte **Exclude** dans le volet droit.
3. Cliquez sur **Exclude** (Exclure).

Pour inclure un nouveau groupe de règles ou plusieurs groupes de règles avec les règles personnalisées chargées ou un groupe de règles précédemment exclus :

1. Cliquez sur **Ajouter** (+) à côté de la liste déroulante du filtre de groupes de règles.
 2. Choisissez tous les groupes de règles que vous souhaitez ajouter en cochant la case à côté de ceux-ci.
 3. Cliquez sur **Save** (Enregistrer).
- Pour un groupe de règles enfant, cliquez sur l'icône sous l'en-tête de colonne **Override** (Remplacer) pour voir le journal d'actions de la règle, qui décrit la séquence d'actions de remplacement de règle qui peuvent être affectées en raison de remplacements de politique et de groupe de base pour une règle de prévention des intrusions. Les actions liées aux règles peuvent être obtenues à partir des configurations de politiques de base ou du remplacement de groupe d'utilisateurs. Le remplacement de groupe d'utilisateurs a la priorité entre les deux; La priorité fait référence à l'action finale remplacée qui est affectée au groupe de règles.
 - Cliquez sur le nombre de règles (nombre) sous l'en-tête de colonne **Nombre de règles** pour afficher un résumé des règles qui font partie du groupe de règles.

Étape 7 **Recommendations** (Recommandations) : cliquez sur la couche **Recommendations** (Recommandations) si vous souhaitez générer et appliquer les règles recommandées par Cisco. Les recommandations utilisent la base de données hôte pour activer ou désactiver les règles, en fonction des vulnérabilités connues.

Étape 8 **Rule Overrides** (Remplacements de règles) : cliquez sur la couche **Rule Overrides** (Remplacements de règles) pour choisir l'un des préréglages afin d'afficher les règles, qui sont définies comme suit : alerter, bloquer, désactiver, remplacer, réécrire, transmettre, abandonner ou rejeter.

- La colonne **Définir par** indique l'état défini par défaut (politique de base) ou l'état de règle modifié par les remplacements de groupe, les remplacements de règles ou les recommandations. La colonne **Set By** dans **All Rules** (Définir par dans Toutes les règles) (dans le volet gauche) affiche le suivi des actions de remplacement des règles en fonction de l'ordre de priorité. L'ordre de priorité des actions liées aux règles est Remplacement de la règle > Recommendations > Remplacement de groupe > Politique de base.
- Modifier **Rule Action** (Action de règle) : pour modifier des actions de règles, choisissez l'une des options suivantes :
 - Modification en bloc : choisissez une ou plusieurs règles, puis choisissez l'action requise dans la liste déroulante **Rule Action** (Action de règle); puis cliquez sur **Save** (Enregistrer).



Remarque

Les modifications en bloc d'actions de règle sont prises en charge uniquement pour les 500 premières règles.

- Single Rule Edit (modification d'une règle unique) : choisissez l'action pour la règle dans la liste déroulante de la colonne **Rule Action** (Actions de règle).

Les actions découlant d'une règle sont :

- **Block** (Blocage) : génère un événement, bloque le paquet correspondant actuel et tous les paquets suivants dans cette connexion.
- **Alert** (Alerte) : génère uniquement un événement pour le paquet correspondant, sans abandonner le paquet ni la connexion.
- **Disable** (Désactiver) : ne correspond pas au trafic avec cette règle. Aucun événement n'est généré.
- **Revert to default** (Revenir aux valeurs par défaut) : restaure l'action par défaut du système.
- **Pass** (Réussite) : aucun événement généré, ce qui permet au paquet de passer sans évaluation supplémentaire par les règles Snort suivantes.



Remarque

L'action Pass est disponible uniquement pour les règles personnalisées et non pour les règles fournies par le système.

- **Drop** (Abandonner) : génère un événement, abandonne le paquet correspondant et ne bloque pas le trafic additionnel dans cette connexion.
- **Reject** : génère un événement, abandonne le paquet correspondant, bloque le trafic additionnel dans cette connexion et envoie les messages réinitialisation TCP ou port ICMP inaccessible aux hôtes source et de destination.

Behavior of reject in different firewall modes and IP address or source or destination in relation to Client or Server (Comportement de rejet dans différents modes de pare-feu et adresse IP, ou source ou destination par rapport au client ou au serveur) : Snort envoie des paquets RST au client et au serveur dans le cas d'interfaces routées, en ligne et pontées. Snort envoie deux paquets RST. Le paquet RST dans la direction du client aura la source définie sur l'adresse IP du serveur et la destination définie sur l'adresse IP du client. Le paquet RST dans la direction du serveur aura la source définie sur l'adresse IP du client et la destination définie sur l'adresse IP du serveur.

- **Rewrite** (Réécrire) : génère des événements et remplace le contenu des paquets en fonction de l'option de remplacement dans la règle.

Pour la journalisation des actions liées aux règles IPS, consultez [Journalisation des actions liées aux règles, à la page 9](#).

S'il y a une règle **React** (Réagir), elle est convertie en action d'alerte.

Étape 9

Cliquez sur la couche **Summary** (résumé) pour obtenir une vue globale des modifications actuelles apportées à la politique. La page de résumé de la politique contient les informations suivantes :

- Répartition des règles de la politique, c'est-à-dire les règles actives, les règles désactivées, etc.
- Option d'exportation de la politique et de génération d'un rapport sur la politique de prévention des intrusions.
- Renseignements sur la politique de base.
- Générer des recommandations
- Les remplacements de groupe répertorient les groupes que vous avez remplacés.
- Remplacements de règles qui affiche la liste des règles que vous avez remplacées.
- Dans la couche **Summary** (Résumé), cliquez sur l'icône ? pour ouvrir une fenêtre contextuelle qui explique les concepts de superposition de Snort.

Pour modifier la politique de base, consultez [Modifier la politique de base d'une politique de prévention des intrusions, à la page 10](#).



Remarque

Vous pouvez accéder à **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**, puis cliquer sur l'onglet **Snort 3 Toutes les règles** et parcourir tous les groupes de règles d'intrusion. Le groupe de règles parent répertorie les groupes enfants associés et le nombre de règles.

Prochaine étape

Déployer les modifications de configuration. Voir [Déploiement des modifications de configuration](#).

Rapport de groupe de règles

Le rapport de groupe de règles est une fonction d'analyse de sécurité qui

- reflète les groupes de règles dans les incidents d'intrusion générés,

- comprend l'identification des tactiques et techniques MITRE, et
- fournit des colonnes dédiées pour les groupes de règles MITRE et non-MITRE dans les affichages des incidents d'intrusion.

Accès au rapport de groupe de règles et champs

Pour accéder aux incidents d'intrusion, dans Firewall Management Center, rendez-vous à **Analysis (Analyse) > Intrusions > Events (Événements)**, et cliquez sur l'onglet **Table View of Events** (Tableau des événements). Vous pouvez également afficher les champs d'incident d'intrusion dans la visionneuse d'**événements unifiés**. Dans l'onglet **Analysis** (analyse), cliquez sur **Unified Events** (événements unifiés).

Dans la page **Intrusion Events** (Incidents d'intrusion), les champs suivants sont ajoutés pour les rapports sur les groupes de règles. Notez que vous devez activer explicitement les colonnes mentionnées.

- MITRE ATT&CK
- Groupe de règles

Pour en savoir plus sur ces champs, consultez la section *Champs d'incidents d'intrusion* dans le *Guide d'administration de Cisco Secure Firewall Management Center, version 7.3*.

Journalisation des actions liées aux règles

À partir de la version Firewall Management Center 7.2.0, sur la page **Intrusion Events** (Incidents 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, les tableaux présentent les événements affichés dans la colonne **Inline Result** (Résultat en ligne) de la fenêtre **Intrusion Events** (Événements d'intrusion) et dans la colonne **Action** pour **Intrusion Event Type** (Type d'incident d'intrusion) dans la fenêtre **Unified Events** (Événements unifiés).

Action IPS pour Snort 3	Résultat en ligne : Firewall Management Center 7.1.0 ou versions antérieures	Résultat en ligne : Firewall Management Center 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 « **Would Rewrite** » (Réécrivait).
- L'action **Rewrite** (Réécriture) est également affichée comme **Would Rewrite** (Réécrivait) si l'option Replace (Remplacer) est spécifiée, mais que la politique IPS est en mode Detection (Détection) ou que le périphérique est en mode Inline-TAP (TAP en ligne) ou Passive (Passif).

**Remarque**

En cas de compatibilité ascendante (Firewall Management Center 7.2.0 assurant la gestion d'un périphérique Firewall 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 Firewall Management Center 7.1.0 s'appliquent.

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

Modifiez la politique de base pour utiliser une autre politique fournie par le système ou personnalisée comme base pour la configuration de votre 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 **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#).

Afficher le mappage de politique de base Snort 2 et Snort 3

Cette tâche vous permet d'afficher le mappage entre les politiques de prévention des intrusions Snort 3 et Snort 2.

**Remarque**

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Procédure

- Étape 1** Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.
- Étape 3** Cliquez sur **IPS Mapping** (Mappage IPS).
- Étape 4** Dans la boîte de dialogue **IPS Policy Mapping** (Mappage de politique IPS), cliquez sur **View Mappings** (Afficher les mappages) pour afficher le mappage de la politique de prévention des intrusions de Snort 3 à Snort 2.
- Étape 5** Cliquez sur **OK**.

Synchroniser les règles de Snort 2 avec celles de Snort 3

Cette tâche permet de s'assurer que les paramètres de remplacement de règles Snort 2 et les règles personnalisées sont répliqués sur Snort 3, vous permettant de commencer avec une couverture similaire lors de la transition entre les versions.

Pour s'assurer que les paramètres et les règles personnalisées de la version Snort 2 sont conservés et transférés dans Snort 3, Firewall Management Center fournit la fonctionnalité de synchronisation. La synchronisation aide les paramètres de règles de Snort 2 à remplacer les règles et les paramètres de règles personnalisées, que vous avez peut-être modifiés et ajoutés au cours des derniers mois ou années, pour être répliqués sur la version Snort 3. Cet utilitaire sert à synchroniser la configuration de la politique de Snort 2 avec la version de Snort 3 pour commencer avec une couverture semblable.

**Remarque**

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Si Firewall Management Center est mis à niveau de la version 6.7 ou antérieure vers la version 7.0 ou ultérieure, le système synchronise la configuration. S'il s'agit d'une nouvelle version 7.0 ou d'une version ultérieure, vous pouvez effectuer une mise à niveau vers une version ultérieure Firewall Management Center. Le système ne synchronisera aucun contenu pendant la mise à niveau.

Avant de mettre à niveau un appareil vers Snort 3, si des modifications sont apportées à la version de Snort 2, vous pouvez vous servir de cet utilitaire afin d'obtenir la dernière synchronisation de la version de Snort 2 vers la version de Snort 3 et ainsi commencer avec une couverture semblable.

**Remarque**

Lorsque vous passez à Snort 3, gérez la version Snort 3 de la politique de manière indépendante. N'utilisez pas cet utilitaire comme une opération normale.

**Important**

- Seuls les remplacements de règles Snort 2 et les règles personnalisées sont copiés dans Snort 3 et non le contraire. Il se peut que vous ne trouviez pas de mappage individuel de toutes les règles de prévention des intrusions dans Snort 2 et Snort 3. Vos modifications apportées aux actions liées aux règles pour les règles qui existent dans les deux versions sont synchronisées lorsque vous effectuez la procédure suivante.
- La synchronisation *ne migre pas* les paramètres de seuil et de suppression des règles personnalisées ou fournies par le système de Snort 2 vers Snort 3.

Procédure

Étape 1 Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.

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

Étape 3 Cliquez sur **Afficher l'état de synchronisation de Snort 3**

Étape 4 Déterminez la politique de prévention des intrusions désynchronisée.

Étape 5 Cliquez sur l'icône **Sync Désynchronisation de Snort** (→).

**Remarque**

Si les versions Snort 2 et Snort 3 de la politique de prévention des intrusions sont synchronisées, l'icône **Sync** est de couleur bleue **Versions Snort synchronisées** (→).

Étape 6 Lisez le résumé. Téléchargez une copie du résumé, au besoin.

Étape 7 Cliquez sur **Re-Sync** (Resynchroniser).

**Remarque**

- Les paramètres synchronisés ne seront applicables sur le moteur de prévention des intrusions Snort 3 que s'ils sont appliqués sur un périphérique et après un déploiement réussi.
- Les règles personnalisées Snort 2 peuvent être converties vers Snort 3 à l'aide de l'outil fourni par le système. Si vous avez des règles personnalisées Snort 2, cliquez sur l'onglet Custom Rules (Règles personnalisées) et suivez les instructions à l'écran pour convertir les règles. Pour en savoir plus, consultez [Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3](#).

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Gérer les politiques de prévention des intrusions

Cette tâche vous permet d'effectuer des opérations de gestion complètes sur vos politiques de prévention des intrusions, notamment la création, la modification, la suppression, l'exportation, le déploiement et la création de rapports.

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

- le nombre de stratégies de contrôle d'accès et de périphériques utilisant la politique de prévention des intrusions pour inspecter le trafic.
- Indique le domaine dans lequel la politique a été créée.



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion . |
| Étape 2 | <p>Gérez votre politique de prévention des intrusions :</p> <ul style="list-style-type: none"> • 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 Firewall Management Center, cliquez sur Exporter; Reportez-vous à la rubrique <i>Exportation des</i> |

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 [Déploiement des 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 configuration de règles de contrôle d'accès pour effectuer la prévention des intrusions est un mécanisme de sécurité qui

- permet à plusieurs règles de contrôle d'accès dans une stratégie de contrôle d'accès d'être associées aux politiques de prévention des intrusions,
- permet l'inspection de prévention des intrusions pour les règles de contrôle d'accès Allow (autoriser) ou Interactive (bloquer interactif) afin de faire correspondre différents profils d'inspection de prévention des intrusions à différents types de trafic, et
- évalue le trafic avant qu'il n'atteigne sa destination finale sur le réseau.

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.

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

Configurez une règle de contrôle d'accès pour activer l'inspection de prévention des intrusions sur le trafic réseau, afin de détecter et de prévenir les activités malveillantes en fonction des signatures et des politiques de prévention des intrusions.

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

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

Procédure

-
- | | |
|----------------|--|
| Étape 1 | Dans l'éditeur de politique de contrôle d'accès, créez une règle ou modifiez une règle existante; Consultez la rubrique <i>Composants de la règle de contrôle d'accès</i> dans la dernière version du <i>Guide de configuration de Cisco Secure Firewall Management Center</i> . |
| Étape 2 | Assurez-vous que l'action de règle est définie sur Allow (autorisation), Interactive Block (blocage interactif) ou Interactive Block with reset (blocage interactif) avec réinitialisation . |
| Étape 3 | Cliquez sur Inspection . |
| Étape 4 | Choisissez une politique de prévention des intrusions fournie par le système ou personnalisée, ou choisissez Aucun pour désactiver l'inspection de prévention des intrusions pour le trafic qui correspond à la règle de contrôle d'accès. |
| Étape 5 | Si vous souhaitez modifier l'ensemble de variables associé à la politique de prévention des intrusions, choisissez une valeur dans la liste déroulante Ensemble de variables . |
| Étape 6 | Cliquez sur Save (Enregistrer) pour enregistrer la règle. |
| Étape 7 | Cliquez sur Save (Enregistrer) pour enregistrer la politique. |
-

Prochaine étape

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#).

Régler les politiques de prévention des intrusions à l'aide de règles

Cette section fournit des informations sur les règles personnalisées dans Snort 3, les actions liées aux règles de prévention des intrusions, les filtres de notification d'incidents d'intrusion dans une politique de prévention des intrusions, la conversion des règles personnalisées de Snort 2 vers Snort 3 et l'ajout de groupes de règles avec des règles personnalisées à une politique de prévention des intrusions.

Réglage des règles de prévention des intrusions

Le réglage des règles de prévention des intrusions est un processus de configuration qui

- active la modification de l'état des règles pour les règles d'objets partagés, les règles de texte standard et les règles d'inspection,
- contrôle la génération d'incidents et le traitement du trafic en fonction de la configuration des règles, et
- permet le filtrage des règles afin d'afficher des sous-ensembles précis pour les modifications de configuration ciblées.

Configuration de l'état des règles

Vous activez une règle en réglant son état à Alerte ou à Bloquer. L'activation d'une règle permet au système de générer des événements sur le trafic correspondant à la règle. La désactivation d'une règle arrête le traitement de la règle. Vous pouvez également définir votre politique de prévention des intrusions de sorte qu'un ensemble de règles comme Block (Bloquer) génère des événements et abandonne le trafic correspondant.

Vous pouvez filtrer les règles pour afficher un sous-ensemble de règles, ce qui vous permet de sélectionner l'ensemble de règles exact pour lequel vous souhaitez modifier l'état ou les paramètres des règles.

Lorsqu'une règle de prévention des intrusions ou un argument de règle nécessite un inspecteur désactivé, le système l'utilise automatiquement avec sa configuration actuelle, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.



Remarque

Nous vous recommandons de ne pas modifier les règles d'objets partagés et d'activer ou de désactiver ces règles pour votre périphérique Threat Defense. Pour créer des règles Snort personnalisées, contactez le service d'assistance Cisco.

Types de règles de prévention des intrusions

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.

- *les règles de prévention des intrusions*, qui sont subdivisées en *règles d'objets partagés* et en *règles de texte standard*.

- les règles de l'inspecteur, qui sont associées à une option de détection du décodeur de paquets ou à l'un des inspecteurs inclus avec le système.

Attributs et caractéristiques du type de règle

Le tableau suivant résume les attributs de ces types de règles :

Tableau 1 : Types de règles de prévention des intrusions

Type	ID de générateur (GID)	ID Snort (SID)	Source	Puis-je copier?	Puis-je effectuer des modifications?
Règle des objets partagés	3	inférieur à 1,000,000	Cisco Talos Intelligence Group (Talos)	oui	limité
Règle de texte standard	1 (Domaine global ou GID existant)	inférieur à 1,000,000	Talos	oui	limité
	1 000-2 000 (domaine descendant)	1,000,000 ou plus	Créé ou importé par l'utilisateur	Oui	oui
règle de préprocesseur	propre au décodeur ou au préprocesseur	inférieur à 1,000,000	Talos	Non	Non
		1,000,000 ou plus	Généré par le système lors de la configuration des options	Non	Non

Vous ne pouvez pas enregistrer les modifications d'une règle créée par Talos, mais vous pouvez enregistrer une copie d'une règle modifiée en tant que règle personnalisée. Vous pouvez modifier les variables utilisées dans la règle ou les informations d'en-tête de règle (comme les ports source et de destination et les adresses IP). Dans un déploiement multidomaine, les règles créées par Talos appartiennent au domaine global. Les administrateurs des domaines descendants peuvent enregistrer des copies locales des règles, qu'ils peuvent ensuite modifier.

Pour les règles qu'il crée, Talos attribue des états de règles par défaut dans chaque politique de prévention des intrusions par défaut. La plupart des règles de préprocesseur sont désactivées par défaut et doivent être activées si vous souhaitez que le système génère des événements pour les règles de préprocesseur et, dans un déploiement en ligne, abandonne les paquets fautifs.

Règles personnalisées dans Snort 3

Une règle personnalisée dans Snort 3 est une règle de détection d'intrusion qui

- permet aux utilisateurs de créer une détection personnalisée des menaces en important des fichiers de règles locaux avec les extensions `.txt` ou `.rules`,
- appartient à des groupes de règles et peut être inclus dans plusieurs groupes simultanément, et

- reçoit un numéro de règle unique au format `GID:SID:Rev` avec des identifiants générés par le système.

Format du numéro de règle

Lorsque vous créez une règle de prévention des intrusions personnalisée, le système lui attribue un numéro de règle unique, qui a le format `GID:SID:Rev`. Les éléments composant ce numéro sont les suivants :

- **GID** : ID de générateur. Pour les règles personnalisées, il n'est pas nécessaire de préciser le GID. Le système génère automatiquement le GID lors du chargement des règles selon que vous vous trouvez dans le domaine global ou dans un sous-domaine. Pour toutes les règles de texte standard, cette valeur est de 2 000 pour un domaine global.
- **SID** : ID Snort. Indique s'il s'agit d'une règle locale d'une règle système. Lorsque vous créez une règle, attribuez-lui un SID unique.

Les numéros SID des règles locales commencent à 1,000,000 et le SID de chaque nouvelle règle locale est incrémenté de un.
- **Rev** : le numéro de la révision. Pour une nouvelle règle, le numéro de révision est de 1. Chaque fois que vous modifiez une règle personnalisée, le numéro de révision doit être incrémenté de un.

Dans une règle de texte standard personnalisée, vous définissez les paramètres d'en-tête de règle ainsi que les mots-clés et les arguments de la règle. Vous pouvez utiliser les paramètres d'en-tête de règle pour axer la règle de manière à ce qu'elle ne corresponde qu'au trafic utilisant un protocole spécifique et circulant vers ou à partir d'adresses IP ou de ports spécifiques.

Pour vérifier si un SID est activé ou désactivé, consultez les entrées du fichier `snort.lua` situé dans le répertoire `./file-contents/ngfw/var/sf/detection_engines/<ID>/IPS/<ID>`.

- Si le SID est désactivé par défaut, aucune entrée n'est présente dans le fichier.
- Si le SID est activé manuellement, vous noterez la présence d'une entrée **enable:yes**.
- Si le SID est désactivé après avoir été activé manuellement, l'entrée reste dans le fichier et affiche **enable:no**.



Remarque

- Les règles personnalisées Snort 3 ne peuvent pas être modifiées. Assurez-vous que les règles personnalisées comportent un message de classification valide pour `classtype` dans le texte de la règle. Si vous importez une règle sans classification ou avec une mauvaise classification, supprimez et recréez la règle.
- Vous pouvez créer des règles de prévention des intrusions personnalisées dans Snort 3. Cependant, la prise en charge du réglage et de la résolution de problèmes liés à ces règles n'est pas disponible pour le moment.
- Le `classtype` dans une règle Snort attribue une classification à la règle indiquant le type d'attaque associé à un événement. Un niveau de priorité de 1 à 4 est également associé à chaque `classtype`. Cependant, le niveau de priorité de certains `classtypes` sur l'appareil de protection contre les menaces ne correspond pas aux niveaux de priorité de `classtypes` Snort à code source libre qui sont mentionnés dans la [documentation](#) Snort. Par exemple, `tcp-connection` a une priorité de 4 dans Snort à code source libre, tandis qu'une priorité de 3 lui est attribuée sur l'appareil de protection contre les menaces.

Détection de données sensibles

Des données sensibles telles que les numéros de sécurité sociale, les numéros de carte de crédit, les courriels, etc. peuvent être divulgués sur Internet, intentionnellement ou accidentellement. La détection des données sensibles est utilisée pour détecter et générer des événements relatifs à d'éventuelles fuites de données sensibles. Les incidents sont générés uniquement en cas de transfert d'une quantité importante de renseignements personnels identifiables. La détection des données sensibles peut masquer les renseignements nominatifs dans la sortie des événements.

Utilisez l'option d'IPS `sd_pattern` pour détecter et filtrer les renseignements nominatifs. Ces renseignements comprennent les numéros de cartes de crédit, les numéros de sécurité sociale aux États-Unis, les numéros de téléphone et les adresses de courriel. La syntaxe d'une expression régulière (regex) est disponible pour définir vos propres renseignements nominatifs.

L'option `sd_pattern` a les paramètres suivants :

- **Modèle** : paramètre implicite obligatoire qui spécifie l'expression régulière à rechercher dans la PDU. L'expression régulière doit être écrite en syntaxe PCRE.
- **Seuil** : paramètre explicite et facultatif qui spécifie le nombre de correspondances dans la PDU requises pour générer un événement.

L'option de règle `sd_pattern` comme IPS est disponible dans Snort sans exigence pour des inspecteurs supplémentaires. La syntaxe de l'option de règle est la suivante :

```
sd_pattern: "<pattern>"[, threshold <count>];
```

Par exemple :

```
sd_pattern:"credit_card", threshold 2;
```

Il existe cinq modèles intégrés pour les données sensibles. Pour utiliser les schémas intégrés dans le paramètre « pattern », vous devez préciser le nom du type de renseignements nominatifs qui doivent être mis en correspondance, et l'expression régulière nécessaire lui est remplacée. Le nom des renseignements nominatifs et les mappages ou modèles d'expression régulière sont décrits comme suit :

Tableau 2 : Schémas intégrés

Nom des renseignements nominatifs	Schéma
credit_card	<code>\d{4}\d?\d{4}\d?\d{2}\d?\d{2}\d?\d{3,4}</code>
us_social	<code>[0-8]\d{2}-\d{2}-\d{4}</code>
us_social_nodashes	<code>[0-8]\d{8}</code>
Courriel	<code>[a-zA-Z0-9!#\$%&'*/+=?^_`{ }~]+(?:\.[a-zA-Z0-9!#\$%&'*/+=?^_`{ }~]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?</code>
us_phone	<code>(?:\+?1[-.\s]?)?\(?([2-9][0-8]\d)\)?[-.\s]([2-9]\d{2})[-.\s]\d{4}</code>

Le masquage pour les données correspondant à ces schémas ne fonctionne qu'avec les règles fournies par le système ou les schémas intégrés pour les cartes de crédit, les numéros de sécurité sociale américains, les adresses courriel et les numéros de téléphone aux États-Unis. Le masquage ne fonctionne pas pour les règles personnalisées ou les schémas de renseignements nominatifs définis par l'utilisateur. Les règles sont disponibles dans le paquet de sécurité allégé (LSP) pour les données sensibles, gid:13. Par défaut, ils ne sont activés dans aucune politique fournie par le système.

Les règles de données sensibles dans LSP couvrent tous les modèles intégrés et ont les valeurs de seuil suivantes :

- credit_card: 2
- us_social: 2
- us_social_nodashes: 20
- email: 20
- us_phone: 20

Vous pouvez utiliser l'option `sd_pattern` pour créer des règles personnalisées et modifier les règles existantes. Pour ce faire, utilisez l'interface de politique de prévention des intrusions Snort 3.

Exemple de règle avec `sd_pattern` avec un modèle et un seuil personnalisés :

```
alert tcp (sid: 1000000001; sd_pattern:"[\\w-\\.]+@[\\w-]+\\.\\.[\\w-]{2,4}",threshold 4; msg: "email, threshold 4")
```

Exemples

Exemple de règles personnalisées utilisant la détection des données sensibles :

Règle avec modèle intégré

```
alert tcp (
    msg:"SENSITIVE-DATA Email";
    flow:only_stream;
    pkt_data;
    sd_pattern:"email", threshold 5;
    service:http, smtp, ftp-data, imap, pop3;
    gid:2000;
    sid:1000001;
)
```

Règle avec modèle personnalisé

```
alert tcp (
    msg:"SENSITIVE-DATA US phone numbers";
    flow:only_stream;
    file_data;
    sd_pattern:"+?3?8?(0[\\s\\.-]\\d{2}[\\s\\.-]\\d{3}[\\s\\.-]\\d{2}[\\s\\.-]\\d{2})", threshold
2;
    service:http, smtp, ftp-data, imap, pop3;
    gid:2000;
    sid:1000002;
)
```

Voici quelques autres exemples de règles IPS Snort complètes avec des schémas de données sensibles intégrés :

- alert tcp (sid:1; msg:"Credit Card"; sd_pattern:"crédit_card", seuil 2;)
- alert tcp (sid:2; msg:"US Social Number"; sd_pattern:"us_social", threshold 2;)
- alert tcp (sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes", threshold 2;)
- alert tcp (sid:4; msg:"US Phone Number"; sd_pattern:"us_phone", threshold 2;)
- alert tcp (sid:5; msg:"Email"; sd_pattern:"email", threshold 2;)

La désactivation du masquage des données n'est pas prise en charge dans Cisco Secure Firewall Management Center et Cisco Secure Firewall Device Manager.

Pour en savoir plus sur l'ajout de règles personnalisées aux groupes de règles, consultez [Ajouter des règles personnalisées aux groupes de règles](#), à la page 32.

Afficher les règles de prévention des intrusions Snort 3 dans une politique de prévention des intrusions

Cette tâche vous permet d'afficher et d'interagir avec les règles de prévention des intrusions Snort 3 dans une politique de prévention des intrusions, vous permettant de gérer les paramètres d'affichage des règles et d'accéder aux informations détaillées sur les règles.

Vous pouvez régler l'affichage des règles dans la politique de prévention des intrusions. Vous pouvez également afficher les détails d'une règle spécifique pour voir les paramètres de la règle, la documentation de la règle et d'autres caractéristiques de la règle.

Procédure

-
- Étape 1** Choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Cliquez sur **Version Snort 3** à côté de la politique.
- Étape 3** Lors de l'affichage des règles, vous pouvez :

- Filtrer les règles.
- Choisir un groupe de règles pour afficher les règles associées à ce groupe.
- Afficher les détails d'une règle de prévention des intrusions.
- Afficher les commentaires des règles.
- Afficher la documentation de la règle.

Consultez [Modification des politiques de prévention des intrusions Snort 3](#), à la page 4 pour en savoir plus sur l'exécution de ces tâches.

Actions des règles de prévention des intrusions

Une action de règle de prévention des intrusions est un mécanisme de configuration de politiques qui

- active ou désactive les règles dans les politiques de prévention des intrusions individuelles,
- spécifie l'action entreprise par le système si les conditions surveillées déclenchent la règle, et
- hérite des actions par défaut de la politique de base utilisée lors de la création de la politique de prévention des intrusions.

Comportement de l'action par défaut

Le groupe Intelligence Cisco Talos (Talos) définit l'action par défaut de chaque règle de prévention des intrusions et d'inspecteur dans chaque politique par défaut. Par exemple, une règle peut être activée dans la politique par défaut de Sécurité avant la connectivité et désactivée dans la politique par défaut de Connectivité

avant la sécurité. Talos utilise parfois une mise à jour de règle pour modifier l'action par défaut d'une ou plusieurs règles dans une politique par défaut. Si vous autorisez les mises à jour de règles à mettre à jour votre politique de base, vous autorisez également la mise à jour de règles à modifier l'action par défaut d'une règle de votre politique lorsque l'action par défaut change dans la politique par défaut que vous avez utilisée pour créer votre politique (ou dans la politique par défaut sur laquelle elle est basée). Notez, cependant, que si vous avez modifié l'action de règle, la mise à jour de la règle ne remplace pas votre modification.

Lorsque vous créez une règle de prévention des intrusions, elle hérite des actions par défaut des règles de la politique par défaut que vous utilisez pour créer votre politique.

Options d'actions liées aux règles de prévention des intrusions

Dans une politique de prévention des intrusions, vous pouvez définir l'action d'une règle à des valeurs spécifiques qui déterminent la manière dont le système répond au trafic correspondant.

Alerte

Vous souhaitez que le système détecte une tentative de prévention des intrusions spécifique et génère un incident d'intrusion lorsqu'il trouve le trafic correspondant. Lorsqu'un paquet malveillant traverse votre réseau et déclenche la règle, le paquet est envoyé à sa destination et le système génère un incident d'intrusion. Le paquet malveillant atteint sa cible, mais vous en êtes averti par la journalisation des événements.

Bloquer

Vous souhaitez que le système détecte une tentative de prévention des intrusions spécifique, abandonne le paquet contenant l'attaque et génère un incident d'intrusion lorsqu'il trouve le trafic correspondant. Le paquet malveillant n'atteint jamais sa cible et vous en êtes averti par la journalisation des événements.

Désactiver

Vous ne voulez pas que le système évalue le trafic correspondant.



Remarque

Choisissez les options **Alerte** ou **Bloquer** pour activer la règle. Choisir **Désactiver** désactive la règle.

Nous vous recommandons **vivement** de ne pas activer toutes les règles d'intrusion dans une politique de prévention des intrusions. Les performances de votre périphérique géré sont susceptibles de se dégrader si toutes les règles sont activées. Au lieu de cela, ajustez votre ensemble de règles pour qu'il se conforme le plus possible à votre environnement réseau.

Définir une action de règle de prévention des intrusions

Définissez des actions de règles de prévention des intrusions pour contrôler la façon dont le système répond aux menaces détectées, vous permettant de configurer des règles pour alerter ou bloquer des tentatives d'intrusion spécifiques.

Les états des règles de prévention des intrusions sont propres à la politique.

Procédure

Étape 1 Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.

Étape 2 Cliquez sur **Snort 3 Version** à côté de la politique que vous souhaitez modifier.



Astuces

Cette page affiche le nombre total de :

- Règles désactivées
- Règles activées définies sur Alerte
- Règles activées définies sur Blocage
- Règles remplacées

Étape 3 Choisissez la ou les règles pour lesquelles vous souhaitez définir l'action de la règle.

Étape 4 Choisissez une des actions liées à une règle dans la liste déroulante **Rule Action** (Actions des règles). Consultez [Modification des politiques de prévention des intrusions Snort 3, à la page 4](#) pour plus d'informations sur les différentes actions de règle.

Étape 5 Cliquez sur **Save** (Enregistrer).

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Filtres de notification d'incident d'intrusion dans une politique de prévention des intrusions

Un filtre de notification d'incident d'intrusion dans une politique de prévention des intrusions est un mécanisme de sécurité qui

- détermine l'importance d'un événement en fonction de la fréquence d'occurrence ou des adresses IP source et de destination,
- permet aux administrateurs de préciser des seuils pour le moment où les événements nécessitent votre attention, et
- empêche le système de se submerger en limitant les notifications pour les attaques généralisées.

Scénarios de filtrage des notifications d'événement

L'importance d'un incident d'intrusion peut être fonction de sa fréquence ou de l'adresse IP source ou de destination. Dans certains cas, vous pouvez ne pas vous soucier d'un événement tant qu'il ne se produit pas un certain nombre de fois. Par exemple, vous pourriez ne pas être concerné si quelqu'un tente de se connecter à un serveur avant d'échouer un certain nombre de fois. Dans d'autres cas, vous n'aurez peut-être besoin que de quelques occurrences pour savoir qu'il y a un problème généralisé. Par exemple, si une attaque DoS est lancée contre votre serveur Web, vous n'aurez peut-être besoin de voir que quelques occurrences d'un incident d'intrusion pour savoir que vous devez corriger la situation. Votre système est dépassé lorsqu'il reçoit des centaines du même événement.

Seuils d'incidents d'intrusion

Le seuil d'incident d'intrusion est un paramètre de configuration qui

- limite le nombre de fois où le système enregistre et affiche un incident d'intrusion, en fonction du nombre de fois où l'événement est généré au cours d'une période donnée,
- vous évite d'être submergé par un grand nombre d'événements identiques.
- peut être défini par règle d'objet partagé, règle de texte standard ou règle d'inspecteur.

Définir les seuils d'incidents d'intrusion

Pour définir un seuil, spécifiez d'abord le type de seuil.

Tableau 3 : Options de seuil

Option	Description
Limite	Consigne et affiche les événements à propos du nombre de paquets spécifiés (spécifiés par la quantité d'arguments) qui déclenchent la règle pendant la période spécifiée. Par exemple, si vous définissez le type sur Limite , le nombre sur 10 et les Secondes sur 60, et que 14 paquets déclenchent la règle, le système arrête de consigner les événements de la règle après avoir affiché les 10 premiers qui se produisent dans la même minute.
Seuil	Journalise et affiche un événement unique lorsque le nombre spécifié de paquets (spécifié par l'argument Nombre) déclenche la règle au cours de la période spécifiée. Notez que le compteur de l'heure redémarre une fois que vous avez atteint le nombre seuil d'événements et que le système enregistre cet événement. Par exemple, vous définissez le type sur Seuil , le Nombre sur 10 et Secondes à 60, et la règle se déclenche 10 fois avant la 33ème seconde. Le système génère un événement, puis réinitialise les compteurs des secondes et du nombre à zéro. La règle se déclenche ensuite 10 autres fois dans les 25 secondes suivantes. Comme les compteurs sont réinitialisés à 0 à la 33ème seconde, le système enregistre un autre événement.
Les deux	Enregistre et affiche un événement une fois par période spécifiée, après qu'un nombre spécifié (le nombre) de paquets déclenche l'application de la règle. Par exemple, si vous définissez Typesur Both (Les deux), Count (Nombre) sur deux et Seconds (Secondes) sur 10, vous obtenez le nombre d'événements suivant : • Si la règle est déclenchée une fois toutes les 10 secondes, le système ne génère aucun événement (le seuil n'est pas atteint) • Si la règle est déclenchée deux fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche pour la deuxième fois). • Si la règle est déclenchée quatre fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche la deuxième fois, et les événements suivants sont ignorés)

Ensuite, spécifiez le suivi, qui détermine si le seuil d'événement est calculé par adresse IP source ou de destination.

Tableau 4 : Options IP de seuil

Option	Description
Source	Calcule le nombre d'instances d'événement par adresse IP source.

Option	Description
Destination	Calcule le nombre d'instances d'événement par adresse IP de destination.

Enfin, spécifiez le nombre d'instances et la période qui définissent le seuil.

Tableau 5 : Options de durée/instance de seuil

Option	Description
Quantité	Le nombre d'instances d'événement par période spécifiée et par adresse IP de suivi requise pour atteindre le seuil.
Secondes	Nombre de secondes qui s'écoulent avant la réinitialisation du nombre. Si vous définissez le type de seuil sur limite , le suivi sur l'adresse IP source , le nombre sur 10 et les secondes sur 10, le système journalise et affiche les 10 premiers événements qui se produisent durant 10 secondes à partir d'un port source donné. Si seulement 7 événements se produisent dans les 10 premières secondes, le système les consigne et les affiche; si 40 événements se produisent dans les 10 premières secondes, le système se connecte et en affiche 10, puis recommence le décompte lorsque la période de 10 secondes est écoulée.

Vous pouvez utiliser le seuillage des incidents d'intrusion seul ou le combiner avec la prévention des attaques basée sur le débit, le mot-clé `detection_filter` ou la suppression des incidents d'intrusion.



Astuces

Vous pouvez également ajouter des seuils à partir de la vue de paquets d'un incident d'intrusion.

Définir un seuil pour une règle de prévention des intrusions dans Snort 3

Définissez un seuil pour qu'une règle de prévention des intrusions contrôle le moment et la fréquence de génération des alertes en fonction des instances d'événement au cours d'une période spécifiée.

Vous pouvez définir un seuil unique pour une règle à partir de la page Rule Detail (Détails de la règle). L'ajout d'un seuil remplace tout seuil existant pour la règle. Le seuil que vous définissez pour une règle de prévention des intrusions est appliqué à chaque flux de paquets. Cependant, la configuration n'est pleinement appliquée que dans le contexte d'un flux unique. Vous pourriez voir plus d'alertes sur différents flux de réseau, mais vous ne verrez pas moins d'alertes que le nombre configuré.

Procédure

- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.
- Étape 2** Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.
- Étape 3** Dans la colonne Configuration des alertes d'une règle de prévention des intrusions, cliquez sur le lien **None (Aucune)**.
- Étape 4** Cliquez sur **Modifier** (✎).
- Étape 5** Dans la fenêtre Alert Configuration (configuration des alertes), cliquez sur l'onglet **Threshold (Seuil)**.
- Étape 6** Dans la liste déroulante **Type (Type)**, choisissez le type de seuil que vous souhaitez définir :

- Choisissez **Limit** pour limiter la notification au nombre spécifié d'instances d'événement par période.
- Choisissez **Threshold** (Seuil) pour fournir une notification pour chaque nombre spécifié d'instances d'événement par période.
- Choisissez **Both** (les deux) pour fournir une notification une fois par période après un nombre spécifié d'instances d'événement.

- Étape 7** Choisissez **Source** ou **Destination** dans le champ **Track By** (Suivre par) pour indiquer si vous souhaitez que les instances d'événement soient suivies par adresse IP source ou de destination.
- Étape 8** Saisissez le nombre d'instances d'événement que vous souhaitez utiliser comme seuil dans le champ **Nombre**.
- Étape 9** Dans le champ **Secondes**, saisissez une valeur numérique spécifiant la période, en secondes, pendant laquelle les instances d'événement sont suivies.
- Étape 10** Cliquez sur **Save** (enregistrer).
- Reportez-vous à la vidéo [Snort 3 Suppression and Threshold](#) (Suppression et seuil Snort 3) pour obtenir de l'aide et des renseignements supplémentaires.

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Afficher et supprimer les seuils d'incidents d'intrusion

Cette tâche vous permet d'afficher les paramètres de seuil existants pour les règles de prévention des intrusions et de les supprimer lorsqu'ils ne sont plus appropriés pour la configuration de votre système.

Pour afficher ou supprimer un paramètre de seuil existant pour une règle, utilisez la vue Rules Details (détails des règles) afin d'afficher les paramètres configurés pour un seuil et voir s'ils sont appropriés pour votre système. Si ce n'est pas le cas, vous pouvez ajouter un nouveau seuil pour remplacer les valeurs existantes.

Procédure

- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.
- Étape 2** Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.
- Étape 3** Choisissez la règle avec un seuil configuré, comme indiqué dans la colonne **Alert Configuration** (Configuration d'alerte) (la colonne **Alert Configuration** affiche **Seuil** comme lien pour la règle).
- Étape 4** Pour supprimer le seuil de la règle, cliquez sur le lien **Threshold** (Seuil) dans la colonne **Alert Configuration** (Configuration d'alerte).
- Étape 5** Cliquez sur **Modifier** (✎).
- Étape 6** Cliquez sur l'onglet **Threshold** (seuil).
- Étape 7** Cliquez sur **Réinitialiser**.
- Étape 8** Cliquez sur **Save** (Enregistrer).

Prochaine étape

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#).

Configuration de la suppression des politiques de prévention des intrusions

La configuration de suppression des politiques de prévention des intrusions est un mécanisme de sécurité qui

- supprime la notification d'incidents d'intrusion lorsqu'une adresse IP spécifique ou une plage d'adresses IP déclenche une règle ou un préprocesseur spécifique,
- élimine les faux positifs en permettant aux règles de se déclencher pour tous les paquets tout en n'affichant que les incidents pour les attaques légitimes, et
- est utile dans des scénarios tels que les serveurs de messagerie qui transmettent des paquets simulant des exploits spécifiques.

Exemple de suppression de serveur de messagerie

Si vous avez un serveur de messagerie qui transmet des paquets qui semblent être une exploitation spécifique, vous pouvez supprimer la notification d'incident pour cet incident lorsqu'il est déclenché par votre serveur de messagerie. La règle se déclenche pour tous les paquets, mais vous ne voyez que les événements des attaques légitimes.

Types de suppression des politiques de prévention des intrusions

Notez que vous pouvez utiliser la suppression des incidents d'intrusion seule ou en combinaison avec la prévention des attaques basée sur le débit, le mot-clé `detection_filter` et le seuillage des incidents d'intrusion.



Astuces

Vous pouvez ajouter des suppressions à partir de la vue de paquets d'un incident d'intrusion. Vous pouvez également accéder aux paramètres de suppression en utilisant la colonne **Configuration d'alerte** de la page de l'éditeur de règles de prévention des intrusions **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**, cliquez sur **Snort 3 toutes les règles**.

Définir la suppression pour une règle de prévention des intrusions dans Snort 3

Cette tâche vous permet de configurer une ou plusieurs suppressions pour une règle de votre politique de prévention des intrusions afin de réduire les faux positifs et de vous concentrer sur les incidents de sécurité pertinents.

Vous pouvez définir une ou plusieurs suppressions pour une règle dans votre politique de prévention des intrusions.

Before you begin

Assurez-vous de créer les objets réseau requis à ajouter pour la suppression de source ou de destination.

Suivez ces étapes pour définir la suppression pour une règle de prévention des intrusions dans Snort 3

Procédure

-
- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.
- Étape 2** Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.
- Étape 3** Cliquez sur le lien **None** (Aucun) dans la colonne **Alert Configuration** (Configuration des alertes) de la règle de prévention des intrusions.
- Étape 4** Cliquez sur **Modifier** (✎).
- Étape 5** Sous l'onglet **Suppressions**, cliquez sur l'icône **Ajouter** (+) à côté de l'une des options suivantes :
- Choisissez **Source Networks** (réseaux sources) pour supprimer les événements générés par les paquets provenant d'une adresse IP source spécifiée.
 - Choisissez **Destination Networks** (réseaux de destination) pour supprimer les événements générés par les paquets allant à une adresse IP de destination spécifiée.
- Étape 6** Sélectionnez l'un des réseaux prédéfinis dans la liste déroulante **Network** (réseau).
- Étape 7** Cliquez sur **Save** (enregistrer).
- Étape 8** (Facultatif) Répétez les étapes 5, 6 et 7, si nécessaire.
- Étape 9** Cliquez sur **Save** (Enregistrer) dans la fenêtre **Alert Configuration**.
-

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Afficher et supprimer les conditions de suppression

Affichez ou supprimez les conditions de suppression existantes pour gérer les notifications d'événement pour des conditions de réseau spécifiques.

Vous souhaitez peut-être afficher ou supprimer une condition de suppression existante. Par exemple, vous pouvez supprimer la notification d'événement pour les paquets provenant d'une adresse IP de serveur de messagerie, car ce serveur transmet normalement des paquets qui ressemblent à des exploits. Si vous désactivez ensuite ce serveur de messagerie et réaffectez l'adresse IP à un autre hôte, vous devez supprimer les conditions de suppression pour cette adresse IP source.

Procédure

-
- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.
- Étape 2** Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.
- Étape 3** Choisissez la règle pour laquelle vous souhaitez afficher ou supprimer les suppressions.
- Étape 4** Cliquez sur **Suppression** dans la colonne **Alert Configuration** (configuration des alertes).
- Étape 5** Cliquez sur **Modifier** (✎).
- Étape 6** Cliquez sur l'onglet **Suppressions**.

- Étape 7** Supprimez la suppression en cliquant sur **Effacer** (X) à côté de la suppression.
- Étape 8** Cliquez sur **Save** (Enregistrer).

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Ajouter des commentaires sur les règles de prévention des intrusions

Ajoutez des commentaires aux règles de votre politique de prévention des intrusions à des fins de documentation et de gestion.

Vous pouvez ajouter des commentaires aux règles de votre politique de prévention des intrusions. Les commentaires ajoutés de cette manière sont spécifiques à la politique. Les commentaires que vous ajoutez à une règle dans une politique de prévention des intrusions ne sont pas visibles dans d'autres politiques de prévention des intrusions.

Procédure

-
- Étape 1** Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Cliquez sur **Snort 3 Version** à côté de la politique que vous souhaitez modifier.
- Étape 3** Dans la partie droite de la page, où toutes les règles sont répertoriées, choisissez la règle pour laquelle vous souhaitez ajouter un commentaire.
- Étape 4** Cliquez sur **Commentaires** (🗨) dans la colonne **Commentaires**.
- Étape 5** Dans le champ **Comments** (Commentaires), saisissez un commentaire pour la règle.
- Étape 6** Cliquez sur **Add comment** (ajouter un commentaire).
- Étape 7** Cliquez sur **Save** (enregistrer).
- Le système affiche un **Commentaires** (🗨) à côté de la règle dans la colonne Commentaires.
-

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Préparer des règles personnalisées pour la conversion de SNORT 3

Avant de passer de Snort 2 à Snort 3, assurez-vous que vous êtes prêt à gérer votre ensemble de règles personnalisées pour Snort 3.

- Si vous utilisez un ensemble de règles d'un fournisseur tiers, communiquez avec ce fournisseur pour confirmer que ses règles seront converties avec succès vers Snort 3 ou pour obtenir un ensemble de règles de remplacement écrit de manière native pour Snort 3.

- Si vous avez des règles personnalisées que vous avez écrites vous-même, familiarisez-vous avec la rédaction des règles de Snort 3 avant la conversion, afin de pouvoir mettre à jour vos règles et optimiser la détection de Snort 3 après la conversion.

En savoir plus sur l'écriture de règles dans Snort 3 :

- <https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html>
- <https://blog.snort.org/2020/10/talos-transition-to-snort-3.html>

Vous pouvez consulter d'autres blogs à l'adresse <https://blog.snort.org/> pour en savoir plus sur les règles Snort 3.



Important

Les paramètres de politique d'analyse de réseau (NAP) de Snort 2 *ne peuvent pas* être copiés dans Snort 3 automatiquement. Les paramètres de Politique d'analyse de réseau (NAP) doivent être répliqués manuellement dans Snort 3.



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3.

Convertissez les règles personnalisées Snort 2 existantes au format Snort 3 mis à jour pour assurer la compatibilité avec les systèmes de détection d'intrusion actuels.

Cette tâche migre les règles personnalisées Snort 2 existantes vers le format Snort 3, vous permettant de conserver vos configurations de règles personnalisées lors de la mise à niveau vers le dernier moteur de détection d'intrusion. Vous pouvez soit importer les règles converties directement, soit les télécharger pour les consulter avant de les importer.

Procédure

- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.
- Étape 2** Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.
- Étape 3** Assurez-vous que **Toutes les règles** est sélectionné dans le volet gauche.
- Étape 4** Cliquez sur la liste déroulante **Tasks (Tâches)** et sélectionnez :
 - (Convertir et importer) **Convert Snort 2 rules and import** (Convertir les règles de Snort 2 et les importer) : pour convertir automatiquement toutes les règles personnalisées Snort 2 dans toutes les politiques de prévention des intrusions vers Snort 3 et les importer dans Firewall Management Center en tant que règles personnalisées Snort 3.

- (Convertir et télécharger) **Convert Snort 2 Rules and download** (Convertir les règles Snort 2 et les télécharger) : pour convertir automatiquement toutes les règles personnalisées de Snort 2 pour toutes les politiques de prévention des intrusions vers Snort 3 et les télécharger dans votre système local.

Étape 5 Cliquez sur **OK**.



Remarque

- Si vous avez sélectionné **Convert and import** à l'étape précédente, alors toutes les règles converties sont enregistrées dans un nouveau groupe de règles **All Snort 2 Converted Global** sous **Local Rules** (Règles locales).
- Si vous avez sélectionné **Convert and download** à l'étape précédente, enregistrez le fichier de règles localement. Vous pouvez consulter les règles converties dans le fichier téléchargé et les téléverser ultérieurement en suivant les étapes décrites dans [Ajouter des règles personnalisées aux groupes de règles, à la page 32](#).

Reportez-vous à la vidéo [Conversion des règles Snort 2 en règles Snort 3](#) pour obtenir de l'aide et des renseignements supplémentaires.

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3

Convertissez les règles personnalisées Snort 2 dans une politique de prévention des intrusions au format Snort 3 pour maintenir la compatibilité avec les environnements Snort 3.

Lors de la migration vers Snort 3, les règles personnalisées Snort 2 existantes doivent être converties pour conserver leurs fonctionnalités. Cette tâche vous permet de convertir des règles personnalisées pour une politique de prévention des intrusions spécifique.

Procédure

- Étape 1** Choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Dans l'onglet **Intrusion Policies** (politiques de prévention des intrusions), cliquez sur **Show Snort 3 Sync status** (Afficher l'état de la synchronisation Snort).
- Étape 3** Cliquez sur l'icône **Sync Désynchronisation de Snort** (🔁) de la politique de prévention des intrusions.



Remarque

Si les versions Snort 2 et Snort 3 de la politique de prévention des intrusions sont synchronisées, l'icône **Sync** est de couleur bleue **Versions Snort synchronisées** (🔄). Cela indique qu'il n'y a aucune règle personnalisée à convertir.

Étape 4 Lisez le résumé et cliquez sur l'onglet **Custom Rules** (Règles personnalisées).

Étape 5 Choisissez :

- **Import converted rules to this policy** (Importer les règles converties dans cette politique) : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les importer dans Firewall Management Center en tant que règles personnalisées Snort 3.
- **Download converted rules** (Télécharger les règles converties) : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les télécharger dans votre système local. Vous pouvez consulter les règles converties dans le fichier téléchargé, puis téléverser le fichier ultérieurement en cliquant sur l'icône de chargement.

Étape 6 Cliquez sur **Re-Sync** (Resynchroniser).

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Ajouter des règles personnalisées aux groupes de règles

Chargez des règles personnalisées pour ajouter des règles Snort 3 créées localement à la liste de toutes les règles disponibles dans le système.

Le téléversement de règles personnalisées dans le Firewall Management Center ajoute les règles personnalisées que vous avez créées localement à la liste de toutes les règles Snort 3.

Procédure

Étape 1 Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Cliquez sur la liste déroulante **Tasks** (Tâches) et sélectionnez :

Étape 4 Cliquez sur **Upload Snort 3 Rules** (Téléverser les règles de Snort 3).

Étape 5 Glissez et déposez le fichier `.txt` ou `.rules` qui contient les règles personnalisées de Snort 3 que vous avez créées.

Étape 6 Cliquez sur **OK**.



Remarque S'il y a des erreurs dans le fichier sélectionné, vous ne pouvez pas continuer. Vous pouvez télécharger le fichier d'erreur et **remplacer le fichier** pour téléverser la version 2 du fichier, après avoir corrigé les erreurs.

Étape 7 Associez des règles à un groupe de règles pour ajouter les nouvelles règles à ce groupe.

Vous pouvez également créer un groupe de règles personnalisées (en cliquant sur le lien **Créer un nouveau groupe de règles personnalisées**), puis ajouter les règles au nouveau groupe.

**Remarque**

S'il n'y a aucun groupe de règles locales, continuez en cliquant sur **Créer un nouveau groupe de règles personnalisées pour continuer**. Saisissez un **nom** pour le modèle et cliquez sur **Save** (Enregistrer).

Étape 8

Choisissez l'une des options suivantes :

- **Merge Rules (Fusionner les règles)** pour fusionner les nouvelles règles que vous ajoutez avec les règles existantes dans le groupe de règles.
- **Replace all rules in the group with file contents** (Remplacez toutes les règles du groupe par le contenu du fichier) pour remplacer toutes les règles existantes par les nouvelles règles que vous ajoutez.

**Remarque**

Si vous avez choisi plusieurs groupes de règles à l'étape précédente, seule l'option **Merge Rules** (Fusionner les règles) est disponible.

Étape 9

Cliquez sur **Next** (suivant).

Consultez le résumé pour connaître les nouveaux ID de règles qui sont ajoutés et téléchargez-le éventuellement.

Étape 10

Cliquez sur **Finish** (terminer).

**Important**

Toutes les règles chargées sont désactivées par défaut. Modifiez leur état au besoin pour vous assurer que les règles sont actives.

Prochaine étape

- Le téléversement de règles personnalisées dans le Firewall Management Center ajoute les règles personnalisées que vous avez créées à la liste de toutes les règles Snort 3. Pour appliquer ces règles personnalisées au trafic, ajoutez et activez ces règles dans les politiques de prévention des intrusions requises. Pour en savoir plus sur l'ajout de groupes de règles avec des règles personnalisées à une politique de prévention des intrusions, consultez [Ajouter des groupes de règles avec des règles personnalisées à une politique de prévention des intrusions](#), à la page 33. Pour en savoir plus sur l'activation des règles personnalisées, consultez [Gérer les règles personnalisées dans Snort 3](#), à la page 34.
- Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Ajouter des groupes de règles avec des règles personnalisées à une politique de prévention des intrusions

Activez les règles personnalisées dans une politique de prévention des intrusions pour appliquer ces règles au trafic réseau.

Les règles personnalisées qui sont téléversées dans le système doivent être activées dans une politique de prévention des intrusions pour appliquer ces règles au trafic. Après avoir téléversé les règles personnalisées

sur Firewall Management Center, ajoutez le groupe de règles avec les nouvelles règles personnalisées dans la politique de prévention des intrusions.

Procédure

-
- | | |
|----------------|--|
| Étape 1 | Choisissez Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion . |
| Étape 2 | Dans l'onglet Intrusion Policies (politiques de prévention des intrusions), cliquez sur la version Snort 3 de la politique de prévention des intrusions. |
| Étape 3 | Cliquez sur Ajouter (+) à côté de la barre de recherche des groupes de règles. |
| Étape 4 | Dans la fenêtre Add Rule Groups (ajouter des groupes de règles), cliquez sur l'icône Flèche Développer (➤) à côté d'un groupe de règles pour développer le groupe de règles local. |
| Étape 5 | Cochez la case à côté du groupe de règles personnalisées téléversé. |
| Étape 6 | Cliquez sur Save (Enregistrer). |
-

Prochaine étape

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#).

Gérer les règles personnalisées dans Snort 3

Cette tâche permet aux règles personnalisées chargées dans les politiques de prévention des intrusions d'appliquer la surveillance des règles au trafic réseau.

Les règles personnalisées qui sont téléchargées dans le système doivent être ajoutées à une politique de prévention des intrusions et activées pour appliquer ces règles au trafic. Vous pouvez activer les règles personnalisées téléchargées pour toutes les politiques ou de manière sélective pour des politiques individuelles.

Before you begin

Suivez les étapes ci-dessous pour activer les règles personnalisées dans une ou plusieurs politiques de prévention des intrusions :

Procédure

-
- | | |
|----------------|--|
| Étape 1 | Choisissez Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions) . |
| Étape 2 | Cliquez sur l'onglet Snort 3 All Rules (toutes les règles Snort 3) . |
| Étape 3 | Développez Règles locales . |
| Étape 4 | Sélectionnez le groupe de règles requis. |
| Étape 5 | Sélectionnez les règles en cochant les cases correspondantes. |
| Étape 6 | Sélectionnez Per Intrusion Policy (par politique de prévention des intrusions) dans la liste déroulante Rule Actions (Actions de règles). |
| Étape 7 | Choisissez : <ul style="list-style-type: none"> • All Policies (toutes les politiques) : pour que toutes les règles à ajouter utilisent les mêmes actions. |

- **Per Intrusion Policy** (par politique de prévention des intrusions) : pour avoir des actions de règle différentes pour chaque politique de prévention des intrusions.

Étape 8

Définissez les actions de règle :

- Si vous avez sélectionné **All Policies** (Toutes les politiques à l'étape précédente, sélectionnez l'action de règle requise dans la liste déroulante **Select Override state** (Sélectionner l'état de remplacement).
- Si vous avez sélectionné **Par politique de prévention des intrusions** à l'étape précédente, sélectionnez l'**action de la règle** en fonction du nom de la politique. Pour ajouter d'autres politiques, cliquez sur **Add Another** (Ajouter une autre).

Étape 9

Ajoutez éventuellement un commentaire dans la zone de texte **Comments** (Commentaires).

Étape 10

Cliquez sur **Save** (Enregistrer).

Prochaine étape

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#).

Supprimer des règles personnalisées

Supprimez les règles personnalisées qui ne sont plus nécessaires de votre configuration de règles de prévention des intrusions pour maintenir un ensemble de règles ordonné et efficace.

Utilisez cette procédure lorsque vous devez supprimer des règles personnalisées de la section Local Rules (règles locales) dans l'interface Snort 3 All Rules. Avant la suppression, toutes les règles doivent être désactivées pour éviter les conflits de configuration.

Procédure**Étape 1**

Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.

Étape 2

Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3

Développez **Local Rules** (règles locales) dans le volet gauche.

Étape 4

Cochez les cases des règles que vous souhaitez supprimer.

Étape 5

Assurez-vous que l'action de règle pour toutes les règles que vous sélectionnez est **Disable** (désactiver).

Si nécessaire, suivez ces étapes pour désactiver l'action de règle pour plusieurs règles sélectionnées :

- Dans la liste déroulante **Rule Actions** (actions liées aux règles), sélectionnez **Per Intrusion Policy** (par politique de prévention des intrusions).
- Sélectionnez le bouton radio **All Policies** (toutes les politiques).
- Sélectionnez **Disable** (désactiver) dans la liste déroulante **Select Override state** (sélectionner l'état de remplacement).
- Cliquez sur **Save** (enregistrer).
- Cochez les cases des règles que vous souhaitez supprimer.

Étape 6

Dans la liste déroulante **Rule Actions** (actions de règles), sélectionnez **Delete** (supprimer).

Étape 7 Cliquez sur **Delete** (supprimer) dans la fenêtre contextuelle Delete Rules (supprimer les règles).

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Supprimer les groupes de règles

Supprimez des groupes de règles pour supprimer les règles de détection d'intrusion indésirables ou obsolètes de la configuration de votre système et maintenir une structure de règles ordonnée.

Avant de supprimer un groupe de règles, vous devez l'exclure de toutes les politiques de prévention des intrusions et désactiver toutes les règles du groupe pour éviter les conflits de système.

Before you begin

Excluez le groupe de règles que vous souhaitez supprimer de toutes les politiques de prévention des intrusions où vous l'avez inclus. Pour savoir comment exclure un groupe de règles d'une politique de prévention des intrusions, consultez [Modification des politiques de prévention des intrusions Snort 3](#), à la page 4.

Suivez les étapes suivantes pour supprimer les groupes de règles :

Procédure

-
- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**.
- Étape 2** Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.
- Étape 3** Développez **Local Rules** (règles locales) dans le volet gauche.
- Étape 4** Sélectionnez le groupe de règles à supprimer.
- Étape 5** Assurez-vous que l'action de règle pour toutes les règles du groupe est **désactivée** avant de continuer.
- Si l'action de règle pour l'une des règles est autre que **Désactivée**, vous ne pouvez pas supprimer le groupe de règles. Si nécessaire, suivez les étapes ci-dessous pour désactiver l'action de règle pour toutes les règles :
- Cochez la case sous la liste déroulante **Rule Actions** (actions liées aux règles) pour sélectionner toutes les règles du groupe.
 - Dans la liste déroulante **Rule Actions** (actions liées aux règles), sélectionnez **Per Intrusion Policy** (par politique de prévention des intrusions).
 - Sélectionnez le bouton radio **All Policies** (toutes les politiques).
 - Sélectionnez **Disable** (désactiver) dans la liste déroulante **Select Override state** (sélectionner l'état de remplacement).
 - Cliquez sur **Save** (enregistrer).
- Étape 6** Cliquez sur **Supprimer** () à côté du groupe de règles.
- Étape 7** Cliquez sur **OK** dans la fenêtre contextuelle Delete Rule Group (supprimer le groupe de règles).
-

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Règles recommandées

Ce chapitre fournit un aperçu des règles recommandées par Cisco Secure Firewall ainsi que la génération et l'application des règles recommandées par Cisco Secure Firewall.

Modifications des règles Snort 3 dans les mises à jour des LSP

Les modifications de règles Snort 3 dans les mises à jour de LSP sont des modifications des règles de prévention des intrusions définies par le système qui

- remplacent les règles existantes par de nouvelles règles pour améliorer les capacités de détection,
- combinent plusieurs règles en une seule règle ou développent une seule règle en plusieurs règles lorsqu'une meilleure détection est possible, et
- suppriment les règles existantes définies par le système pour une meilleure gestion dans le cadre de la mise à jour du LSP.

Pour recevoir des notifications des modifications apportées à des règles définies par le système *remplacées* lors des mises à jour des LSP, assurez-vous que la case **Retain user overrides for deleted Snort 3 rules** (Conserver les remplacements de l'utilisateur pour les règles du Snort 3 supprimées) est cochée.

Pour accéder à la case à cocher **Conservez les dérogations s'appliquant aux utilisateurs pour les règles supprimées dans Snort 3**, cliquez sur **Système** (⚙️) > **Configuration** > **Intrusion Policy Preferences** (**Préférences pour les politiques de prévention des intrusions**).

Par défaut, cette case est cochée. Lorsque cette case est cochée, le système conserve les remplacements de règles cliquez sur l'icône d'engrenage dans les nouvelles règles de remplacement qui sont ajoutées dans le cadre de la mise à jour du LSP. Les notifications s'affichent sous l'onglet **Tâches**, sous l'icône Notifications située à côté de **Système** (⚙️).

Règles conseillées pour Secure Firewall

Les règles recommandées pour Secure Firewall sont des recommandations de règles d'intrusion qui

- ciblent les vulnérabilités associées aux ressources hôtes détectées dans le réseau, telles que les systèmes d'exploitation, les serveurs et les protocoles d'application client,
- vous permettent d'adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé, et
- fournissent des recommandations individuelles pour chaque politique de prévention des intrusions. Elles s'appliquent généralement aux règles de texte standard et aux règles d'objet partagé, mais les recommandations peuvent également inclure des règles d'inspection et de décodeur.

Options de configuration de la recommandation de règle

Lorsque vous générez des recommandations d'état de règles, vous pouvez utiliser les paramètres par défaut ou configurer des paramètres avancés. Les paramètres avancés vous permettent de :

- Redéfinir les hôtes de votre réseau que le système surveille pour détecter les vulnérabilités

- Influencer les règles recommandées par le système en fonction du surdébit des règles
- Préciser s'il faut générer des recommandations pour désactiver les règles

Vous pouvez également choisir d'utiliser les recommandations immédiatement ou de passer en revue les recommandations (et les règles touchées) avant de les accepter.

Choisir d'utiliser les états de règles recommandés ajoute une couche de recommandations Cisco Secure en lecture seule à votre politique de prévention des intrusions, puis choisir de ne pas utiliser les états de règles recommandés supprime la couche.

Vous pouvez planifier une tâche pour générer automatiquement des recommandations en fonction des derniers paramètres de configuration enregistrés dans votre politique de prévention des intrusions.

Les états des règles du système ne modifient pas que vous définissez manuellement, tels que :

- La définition manuelle des états de règles spécifiées *avant* de générer des recommandations empêche le système de modifier les états de ces règles à l'avenir.
- La définition manuelle des états de règles spécifiées *après* la génération de recommandations remplace les états recommandés de ces règles.



Astuces

Le rapport sur les politiques de prévention des intrusions peut inclure une liste de règles avec des états de règles différents de l'état recommandé.

Lorsque vous affichez la page des règles filtrées par les recommandations, ou après avoir accédé à la page Rules (Règles) directement à partir du panneau de navigation ou de la page Policy Information (Renseignements sur les politiques), vous pouvez définir manuellement l'état des règles, trier les règles et effectuer toute autre action disponible dans la page Rules, telle que la suppression de règles, la définition de seuils de règles, etc.



Remarque

Le Cisco Talos Intelligence Group (Talos) détermine l'état approprié de chaque règle dans les politiques fournies par le système. Si vous utilisez une politique fournie par le système comme politique de base et que vous permettez au système de définir vos règles selon l'état de règle recommandé par Cisco Secure Firewall, les règles de votre politique de prévention des intrusions correspondent aux paramètres recommandés pour vos actifs réseau.

Générer de nouvelles recommandations Secure Firewall dans Snort 3

Générez les recommandations Secure Firewall pour créer de nouveaux paramètres de règle recommandés dans Snort 3.

Générez les recommandations de Cisco Secure Firewall pour la politique de prévention des intrusions, puis suivez les étapes répertoriées ici pour créer les nouveaux paramètres de règle recommandés dans Snort 3. Les surcharges de règles sont interprétées comme des **security levels** (niveaux de sécurité) basés sur les politiques de seuil que vous avez sélectionnées dans Snort 3. L'action conseillée dépend du niveau de sécurité sélectionné. S'il est supérieur à la politique de base, la recommandation comprend des actions au-delà de la génération d'événements.

Avant de définir les recommandations de Cisco Secure Firewall, vous devez vous demander lequel des trois points ci-dessous correspond le mieux à l'objectif visé :

- **Protection accrue** : active des règles supplémentaires en fonction des vulnérabilités trouvées dans la base de données hôte et ne désactive aucune règle automatiquement. Cela entraînera probablement un ensemble de règles plus important.
- **Protection ciblée** : active des règles supplémentaires et désactive les règles existantes en fonction des vulnérabilités trouvées dans la base de données hôte. Cela peut augmenter ou diminuer le nombre de règles en fonction des vulnérabilités découvertes.
- **Efficacité élevée** : utilisez l'ensemble de règles actuellement activé et désactivez toutes les règles pour les vulnérabilités que l'on ne trouve pas dans la base de données hôte. Cela se traduira probablement par un ensemble de règles activées plus restreint.

En fonction de la réponse, les actions recommandées sont les suivantes :

- Définissez les recommandations au niveau de sécurité immédiatement supérieur et désélectionnez l'option permettant de désactiver les règles.
- Définissez les recommandations au niveau de sécurité immédiatement supérieur et sélectionnez l'option permettant de désactiver les règles.
- Définissez les recommandations au niveau de sécurité actuel et sélectionnez l'option permettant de désactiver les règles.

Before you begin

Les recommandations de CiscoSecure Firewall comportent les exigences suivantes :

- Assurez-vous que des hôtes sont présents dans le système pour générer des recommandations.
- Les réseaux protégés configurés pour les recommandations doivent être mappés aux hôtes présents dans le système

Suivez ces étapes pour générer de nouvelles recommandations Secure Firewall dans Snort 3

Procédure

-
- | | |
|----------------|--|
| Étape 1 | Choisissez Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion . |
| Étape 2 | Cliquer sur le bouton de la version Snort 3 de la politique de prévention des intrusions. |
| Étape 3 | Cliquez sur la couche Recommendations (Not in Use) pour configurer les recommandations de règles. Cliquez sur Start (Démarrer) . |
- Dans la fenêtre Recommandations de règles de Cisco Secure Firewall, vous pouvez définir les éléments suivants :
- **Security Level** (niveau de sécurité) : cliquez pour sélectionner le niveau de sécurité. Vous pouvez éventuellement cocher la case **Accept Recommendation to Disable Rules** (accepter la recommandation pour désactiver les règles) pour désactiver les règles qui ne sont pas activées au niveau de sécurité d'entrée et dans les réseaux protégés. N'activez cette option que si vous devez supprimer votre ensemble de règles en raison d'un nombre élevé d'alertes ou pour améliorer les performances d'inspection. Les niveaux de sécurité sont les suivants :

- Niveau de sécurité 1 : la connectivité prédomine sur la sécurité

Aucune incidence : aucune nouvelle règle ne sera activée et aucune règle existante ne sera désactivée. Pour augmenter les protections, sélectionner un niveau de sécurité plus élevé.

Sécurité inférieure (la case est cochée) : toutes les règles sont désactivées, à l'exception des règles de l'ensemble de règles Connectivité avant sécurité qui correspondent à des vulnérabilités potentielles sur les hôtes détectés. Il est plutôt recommandé d'ajuster la politique de base.

- Niveau de sécurité 2 : équilibre entre sécurité et connectivité

Aucune incidence : aucune nouvelle règle ne sera activée et aucune règle existante ne sera désactivée. Pour augmenter les protections, sélectionner un niveau de sécurité plus élevé.

Efficacité accrue (la case est cochée) : conserve les règles existantes qui correspondent aux vulnérabilités potentielles sur les hôtes découverts et désactive les règles pour les vulnérabilités introuvables sur le réseau.

- Niveau de sécurité 3 : la sécurité prime sur la connectivité

Sécurité accrue : active des règles supplémentaires qui correspondent aux vulnérabilités potentielles des hôtes découverts, sur la base de l'ensemble de règles de détection maximale.

Sécurité ciblée (la case est cochée) : active des règles supplémentaires qui correspondent aux vulnérabilités des hôtes découverts sur la base du jeu de règles. La sécurité prime sur la connectivité, tout en désactivant les règles existantes qui ne correspondent pas aux vulnérabilités potentielles des hôtes découverts.

- Niveau de sécurité 4 : détection maximale

Sécurité accrue : active des règles supplémentaires qui correspondent aux vulnérabilités potentielles des hôtes découverts, sur la base du jeu de règles. La sécurité prime sur la connectivité.

Sécurité ciblée (la case est cochée) : active des règles supplémentaires qui correspondent aux vulnérabilités des hôtes découverts sur la base du jeu de règles de détection maximale, tout en désactivant les règles existantes qui ne correspondent pas aux vulnérabilités potentielles des hôtes découverts.



Remarque

La détection maximale active un très grand nombre de règles et peut avoir une incidence sur la performance. Nous vous recommandons de vérifier ce paramètre et de le tester avant de le déployer dans un environnement de production.

- **Protected Networks** (réseaux protégés) : spécifie les réseaux surveillés ou les hôtes individuels à examiner pour les recommandations. Vous pouvez sélectionner un ou plusieurs objets système ou réseau définis de façon personnalisée dans la liste déroulante. Par défaut, tous les réseaux IPv4 ou IPv6 sont sélectionnés, si aucune sélection n'est effectuée.



Important

Les recommandations de règles de Cisco Secure Firewall dépendent de la découverte de réseau. Les réseaux protégés s'appliquent à tous les hôtes découverts dans les plages configurées dans votre politique de découverte de réseaux. Pour la version Snort 2, consultez le chapitre [Politiques de découverte du réseau](#) dans le *Guide de configuration du périphérique de Cisco Secure Firewall Management Center*.

Cliquez sur le bouton **Add +** (ajouter) pour créer un nouvel objet réseau de type Hôte ou Réseau et cliquez sur **Enregistrer**.

Étape 4 Générer et appliquer les recommandations :

- **Générer** : génère les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous Règles recommandées (non utilisées).
- **Générer et appliquer** : génère et applique les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous Règles recommandées (en cours d'utilisation).

Les recommandations ont été générées avec succès. Un nouvel onglet de recommandation apparaît avec toutes les règles recommandées avec leurs actions recommandées correspondantes. Des filtres d'action de règle prédéfinis sont également disponibles pour cet onglet, en plus de nouvelles recommandations.

Étape 5 Vous pouvez vérifier les recommandations et choisir de les appliquer.

- **Accepter** : applique les recommandations générées précédemment pour une politique de prévention des intrusions.
- **Actualiser** : régénère et met à jour les recommandations de règles pour une politique de prévention des intrusions.
- **Modifier** : ouvre la boîte de dialogue Recommandations, qui vous permet de fournir les valeurs d'entrée de recommandation, puis de générer les recommandations.
- **Supprimer tout** : rétablit ou supprime les règles recommandées appliquées de la politique et supprime également l'onglet de recommandation.

Sous **Toutes les règles**, il y a une section Recommended Rules (règles recommandées) qui affiche les règles recommandées.



Remarque

L'action finale pour une règle de prévention des intrusions est appliquée en fonction de l'ordre de priorité des actions liées aux règles.

Remplacement de règle > Recommandations générées > Remplacement de groupe > Action par défaut de la politique de base

Pour les recommandations activées, Firewall Management Center considère l'état actuel : remplacements de groupes, politique de base et configurations de recommandation, et l'ordre de priorité des actions est :

réussite > blocage > refus > abandon > réécriture > alerte

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Atténuer les menaces à l'aide du cadre MITRE dans les politiques de prévention des intrusions Snort 3

Cette section décrit comment utiliser le cadre MITRE ATT&CK dans les politiques de prévention des intrusions Snort 3 pour identifier les stratégies et les techniques d'attaque, passer en revue la couverture des règles et améliorer la réduction des menaces.

cadre MITRE

Le cadre MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) est une base de connaissance complète qui

- fournit des observations sur les tactiques, les techniques et les procédures (TTP) distribuées par les groupes de menaces ciblant les systèmes,
- intègre des groupes pour faire référence à des groupes de menaces, des groupes d'activités ou des actions de menace en fonction de l'ensemble de stratégies et de techniques qu'ils utilisent, et
- est compilé sous forme de matrices, chaque matrice représentant un système d'exploitation ou une plateforme particulière.

Chaque technique comprend des renseignements sur l'exécution, les procédures, les défenses, les détections et des exemples du monde réel.



Remarque

Consultez le site <https://attack.MITRE.org> pour obtenir des renseignements supplémentaires sur MITRE ATT&CK.

Le centre de gestion utilise le cadre MITRE ATT&CK pour améliorer la détection et la réponse aux menaces, en incorporant les fonctionnalités suivantes :

- Les incidents d'intrusion comprennent des TTP, ce qui permet aux administrateurs de gérer le trafic avec une plus grande granularité en regroupant les règles en fonction du type de vulnérabilité, du système cible ou de la catégorie de menace.
- Certains événements de programmes malveillants utilisent des TTP, ce qui améliore la capacité à détecter les menaces et à y répondre.
- Les visionneuses d'événements unifiés et classiques affichent les tactiques, les techniques, les graphiques de cycle de vie des attaques et les enrichissements contextuels à partir de la classification Talos. Ces enrichissements comprennent des balises MITRE et une vue hiérarchique des tactiques, techniques et sous-techniques associées. Vous pouvez également filtrer les événements à l'aide des identifiants MITRE.

Avantages du cadre MITRE

Le cadre MITRE offre des avantages de sécurité qui

- permettent aux administrateurs d'agir sur le trafic en fonction des Tactiques, Techniques et Procédures (TTP) MITRE ajoutées aux incidents d'intrusion,

- permettent l'affichage et le traitement du trafic avec plus de granularité grâce à des règles de regroupement par type de vulnérabilité, système cible ou catégorie de menace, et
- offrent la possibilité d'organiser les règles de prévention des intrusions selon le cadre MITRE ATT&CK pour des politiques personnalisées en fonction de tactiques et de techniques d'attaques spécifiques.

Exemple de scénario d'entreprise pour le réseau MITER

Un exemple de scénario d'entreprise pour le réseau MITER est un exemple d'implémentation de la sécurité qui

- utilise Snort 3 comme système principal de détection et de prévention des intrusions pour un grand réseau d'entreprise,
- répond au besoin de mesures de sécurité réseau robustes dans un paysage des menaces en pleine évolution, et
- permet aux administrateurs réseau de déterminer si les politiques configurées trouvent le trafic d'intérêt et font le suivi des groupes d'attaques connus.

Questions de sécurité réseau

Les administrateurs réseau doivent savoir si les attaquants tentent de profiter des faiblesses de leurs systèmes ou applications pour provoquer un comportement imprévu. La faiblesse du système peut être un bogue, un problème ou une vulnérabilité de conception. Les applications peuvent être des sites Web, des bases de données, des services standard, tels que Server Message Block (SMB) ou Secure Shell (SSH), des protocoles d'administration et de gestion des périphériques réseau ou des applications, telles que les serveurs Web et les services associés.

Les observations fournies par le cadre MITRE offrent aux administrateurs une possibilité plus précise de préciser la protection pour des ressources spécifiques et de protéger leur réseau contre des groupes de menaces spécifiques.

Préalables pour le cadre MITRE

Assurez-vous que votre système répond à ces exigences avant de mettre en œuvre le cadre MITRE :

- Vous devez exécuter Secure Firewall Management Center et Secure Firewall Threat Defense version 7.3.0 ou ultérieure avec Snort 3.
- Vous devez avoir au moins une politique de prévention des intrusions. Consultez [Création d'une politique de prévention des intrusions Snort 3 personnalisée](#), à la page 3.

Afficher et modifier votre politique de prévention des intrusions Snort 3

Cette tâche vous permet de personnaliser votre politique de prévention des intrusions Snort 3 en modifiant les groupes de règles, les niveaux de sécurité et d'accéder aux règles recommandées par Cisco pour améliorer les capacités de détection des menaces.

Les politiques de prévention des intrusions Snort 3 utilisent une structure de groupes de règles hiérarchique planifiée par le cadre MITRE. Vous pouvez accéder à des catégories de règles spécifiques et modifier les niveaux de sécurité pour les modifications en bloc ou les actions de règles individuelles. L'éditeur de politiques

fournit plusieurs couches, notamment les remplacements de groupe, les remplacements de règles, les recommandations et les affichages résumés.

Procédure

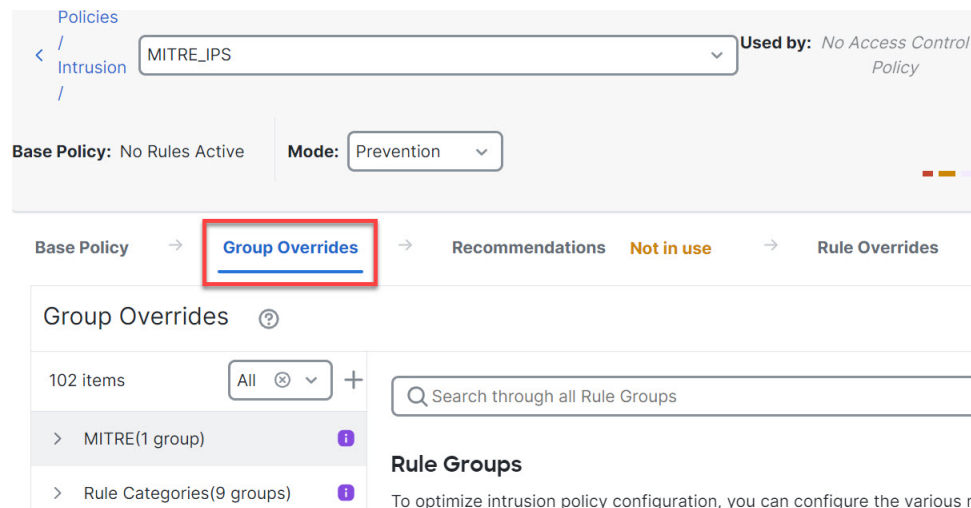
Étape 1 Choisissez **Politiques (Politiques)** > **Access Control heading (En-tête Contrôle d'accès)** > **Intrusion**.

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

- Cliquez sur **Snort 3 Version** (Version Snort 3) à côté de la politique de prévention des intrusions que vous souhaitez afficher ou modifier.
- Fermez le guide de l'assistant Snort qui s'affiche.

Étape 3 Cliquez sur la couche **Group Overrides** (Remplacements de groupe).

Cette couche répertorie toutes les catégories de groupes de règles dans une structure hiérarchique. Vous pouvez accéder au groupe de règles descendant sous chaque groupe de règles.



- Sous **Group Overrides** (Remplacements de groupe), assurez-vous que **All** (Tout) est choisi dans la liste déroulante, de sorte que tous les groupes de règles de la politique de prévention des intrusions correspondante soient visibles dans le volet gauche.

Étape 4 Cliquez sur **MITRE** dans le volet de gauche.



Remarque

Selon vos besoins spécifiques, vous pouvez choisir le groupe de règles **Rule Categories** (Catégories de règles) ou tout autre groupe de règles et ses groupes de sous-règles. Tous les groupes de règles utilisent le cadre MITRE.

a) Sous **MITRE**, cliquez sur **ATT&CK Framework** (Cadre ATT&CK) pour accéder aux détails.

Policies
 < / Intrusion MITRE_IPS Used by: No Access Control Policy
 Base Policy: No Rules Active Mode: Prevention

Base Policy → **Group Overrides** → Recommendations Not in use → Rule Overrides → Summary

Group Overrides ?

102 items All ⊗ +

MITRE(1 group)

ATT&CK Framework(1 group)

Rule Categories(9 groups)

Search through all Rule Groups

MITRE 1 Groups

Security Level

Group Name	Security Level	Override	Rule Count
------------	----------------	----------	------------

b) Sous **ATT&CK Framework**, (Cadre ATT&CK), cliquez sur **Enterprise** (Entreprise) pour le développer.

Policies
 < / Intrusion MITRE_IPS Used by: No Access Control Policy
 Base Policy: No Rules Active Mode: Prevention

Base Policy → **Group Overrides** → Recommendations Not in use → Rule Overrides

Group Overrides ?

102 items All ⊗ +

MITRE(1 group)

ATT&CK Framework(1 gr...)

Enterprise(13 groups)

Rule Categories(9 groups)

Search through all Rule Groups

MITRE / ATT&CK Framework 1 Groups

Group Name	Security Level	Override
------------	----------------	----------

c) Cliquez sur l'icône **Modifier** (✎) à côté du **niveau de sécurité** du groupe de règles pour apporter des modifications en bloc à tous les niveaux de sécurité de groupe de règles associés dans la catégorie du groupe de règles **Enterprise**.

Group Overrides ?

102 items All (selected) +

Search through all Rule Groups

MITRE / ATT&CK Framework 1 Groups

Security Level 4

Group Name	Security Level	Override	Rule Count
------------	----------------	----------	------------

- d) Dans la fenêtre **Edit Security Level** (Modifier le niveau de sécurité), choisissez un **Security Level** (Niveau de sécurité) (dans cet exemple, **3**), puis cliquez sur **Save** (Enregistrer).

Edit Security Level ?

Bulk Group Security Level

Impacts 34 groups. This action will change the security level of all leaf groups within this group category.

Higher security with more detections for administrators who are willing to tolerate some network latency and low level of false positives, in an effort to catch more attacks

Revert to default

Cancel

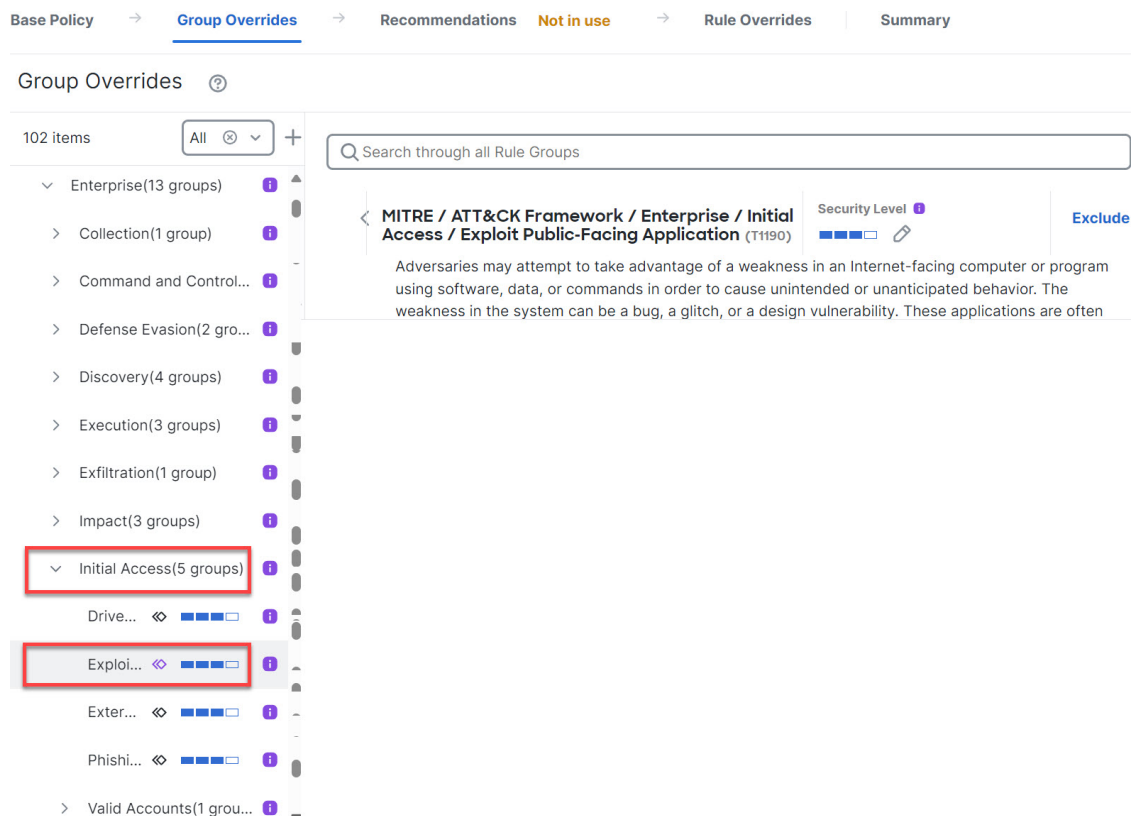
Save

Étape 5

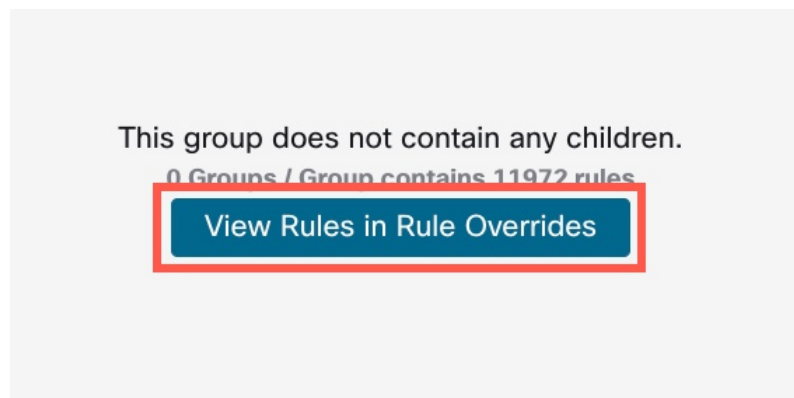
Sous **Enterprise** (Entreprise), cliquez sur **Initial Access** (Accès initial) pour le développer.

Étape 6

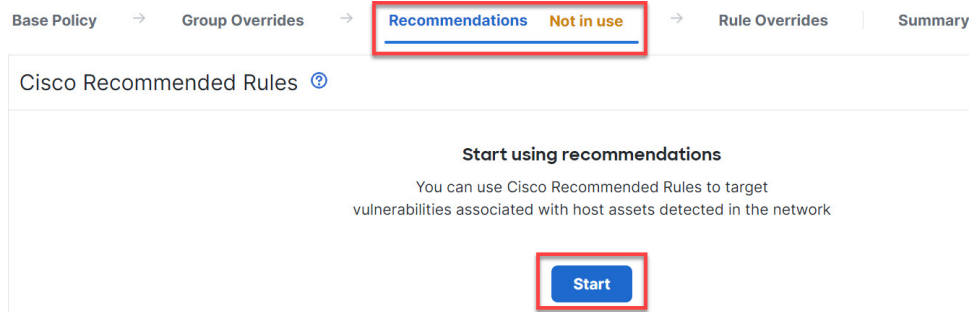
Sous **Initial Access** (Accès initial), cliquez sur **Exploit Public-Facing Application** (Exploiter une application accessible au public), qui est le dernier groupe de règles enfant.

**Étape 7**

Cliquez sur **View Rules** (Afficher les règles) dans Rule Overrides (Remplacements de règles) pour afficher les règles disponibles, leurs détails et leurs actions. Vous pouvez modifier les actions découlant d'une ou de plusieurs règles dans la couche **Rule Overrides** (Remplacements de règles).

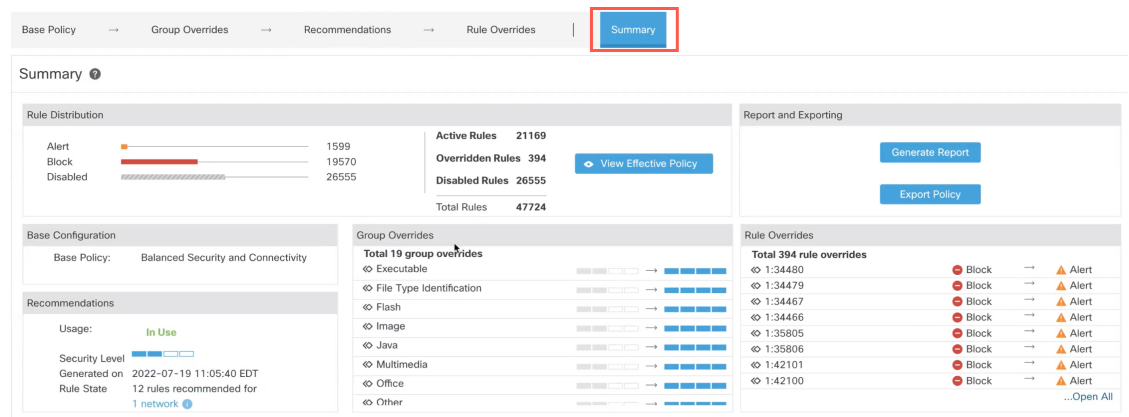
**Étape 8**

Cliquez sur la couche **Recommendations** (Recommandations), puis sur **Start** (Démarrer) pour commencer à utiliser les règles recommandées par Cisco. Vous pouvez utiliser les règles de prévention des intrusions recommandées par Cisco pour cibler les vulnérabilités associées aux ressources hôtes détectées dans le réseau. Pour en savoir plus, consultez [Générer de nouvelles recommandations Secure Firewall dans Snort 3](#), à la page 38.



Étape 9

Cliquez sur la couche **Summary** (résumé) pour obtenir une vue globale des modifications actuelles apportées à la politique. En fonction des remplacements de règles, des modifications de niveau de sécurité et de la génération de règles recommandées par Cisco, vous pouvez afficher la répartition des règles de la politique, les remplacements de groupe, les remplacements de règles, les recommandations de règles et des détails supplémentaires pour vérifier vos modifications.



Prochaine étape

Déployez votre politique de prévention des intrusions pour détecter et consigner les incidents déclenchés par les règles Snort. Consultez [Déploiement des modifications de configuration](#).

Afficher les incidents d'intrusion

Cette tâche vous permet d'afficher les techniques MITRE ATT&CK et les groupes de règles associés aux incidents d'intrusion, en fournissant un contexte de sécurité et un mappage des modèles d'attaque pour une meilleure analyse des menaces.

Vous pouvez afficher les techniques MITRE ATT&CK et les groupes de règles dans les incidents d'intrusion sur les pages **Classic Event Viewer** (Visionneuse d'événements classique) et **Unified Event Viewer** (Visionneuse d'événements unifiés). Talos fournit des mappages à partir des règles Snort (GID:SID) vers les techniques et les groupes de règles MITRE ATT&CK. Ces mappages sont installés dans le cadre du paquet de sécurité allégé (LSP).

Procédure

Étape 1 Cliquez sur **Analysis** (Analyse) et sélectionnez **Events** (Événements) sous **Intrusions**.

Étape 2 Cliquez sur l'onglet **Table View of Events** (Vue de tableau des événements).

Events By Priority and Classification (switch workflow)

No Search Constraints (Edit Search)

2025-01-12 13:30:29 - 2025-01-12 14:45:19 Expanding

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

☐	Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP
☐	2025-01-12 14:43:19	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1
☐	2025-01-12 14:43:19	low	Unknown Target	Alert		0.0.0.0		224.0.0.1
☐	2025-01-12 14:43:19	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1
☐	2025-01-12 14:41:14	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1

Étape 3 Sous **MITRE ATT&CK**, vous pouvez voir les techniques utilisées pour un incident d'intrusion. Cliquez sur **1 Technique** pour afficher les techniques MITRE ATT&CK.

Access Control Policy	Access Control Rule	Network Analysis Policy	MITRE ATT&CK	Rule Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

Dans cet exemple, **Exploit Public-Facing Application** (Exploiter une application publique) est la technique.

MITRE ATT&CK Techniques

- Enterprise
 - Initial Access
 - Exploit Public-Facing Application

Close

Access Control Rule	Network Analysis Policy	MITRE ATT&CK
TestRuleFile	Simple NAP Policy	1 Technique
TestRuleFile	Simple NAP Policy	
TestRuleFile	Simple NAP Policy	
TestRuleFile	Simple NAP Policy	
TestRuleFile	Simple NAP Policy	

Étape 4 Cliquez sur **Close** (Fermer).

Étape 5 Cliquez sur **Analysis** (Analyse) et sélectionnez **Unified Events** (Événements unifiés).

Étape 6 Si elle n'est pas activée, cliquez sur l'icône du sélecteur de colonne pour activer les colonnes **MITRE ATT&CK** et **Rule Group** (Groupe de règles).

The screenshot shows a table of events with columns: Time, Event Type, Rule, Access Control Policy, Device, and MITRE ATT&CK. A 'Column set' dialog is open, showing a search for 'mitre' and a selection of 'MITRE ATT&CK'. The 'Apply' button is highlighted.

Time	Event Type	Rule	Access Control Policy	Device	MITRE ATT&CK
2025-01-12 14:55:49	Connection	AC_with_security_intelligen..	AC_with_security_intelligen..		
2025-01-12 14:55:49	Intrusion	AC_with_security_intelligen..	AC_with_security_intelligen..		
2025-01-12 14:55:49	Intrusion	AC_with_security_intelligen..	AC_with_security_intelligen..		
2025-01-12 14:55:49	Connection	AC_with_security_intelligen..	AC_with_security_intelligen..		
2025-01-12 14:55:49	Intrusion	AC_with_security_intelligen..	AC_with_security_intelligen..		
2025-01-12 14:53:44	Connection	AC_with_security_intelligen..	AC_with_security_intelligen..		
2025-01-12 14:53:44	Intrusion	AC_with_security_intelligen..	AC_with_security_intelligen..		

Étape 7

Dans cet exemple, l'incident d'intrusion est déclenché par un événement mappé à un groupe de règles. Cliquez sur **1 Group** (1 groupe) sous la colonne **Rule Group** (Groupe de règles).

The screenshot shows a table of events with columns: Time, Event Type, Device, MITRE ATT&CK, and Rule Group. A 'Click to view groups' button is highlighted under the 'Rule Group' column.

Time	Event Type	Device	MITRE ATT&CK	Rule Group
2022-07-19 11:19:02	Intrusion	192.168.7.115		1 Group
2022-07-19 11:18:59	Connection	192.168.7.115		
2022-07-19 11:18:59	Connection	192.168.7.115		

Étape 8

Vous pouvez afficher **Protocol** (Protocole), qui est le groupe de règles parent, et le groupe de règles DNS en dessous. Choisissez **Protocol (Protocole)** > **DNS** pour rechercher tous les incidents d'intrusion qui ont au moins un groupe de règles.

The screenshot shows a table of events with columns: Time, Event Type, Device, MITRE ATT&CK, and Rule Group. A search for 'Protocol' and 'DNS' is shown in the 'Rule Group' column.

Time	Event Type	Device	MITRE ATT&CK	Rule Group
2022-07-19 11:19:02	Intrusion	192.168.7.115		1 Group
2022-07-19 11:18:59	Connection	192.168.7.115		
2022-07-19 11:18:59	Connection	192.168.7.115		
2022-07-19 11:18:59	Connection	192.168.7.115		
2022-07-19 11:18:59	Connection	192.168.7.115		

Les résultats de la recherche sont affichés.

The screenshot shows a table of events with columns: Time, Event Type, Device, MITRE ATT&CK, Rule Group, and Snort ID. A search for 'Protocol' and 'DNS' is shown in the 'Rule Group' column.

Time	Event Type	Device	MITRE ATT&CK	Rule Group	Snort ID
2022-07-19 11:19:08	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:07	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:03	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:02	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:59	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:38	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:35	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:31	Intrusion	192.168.7.115		1 Group	1:254:16

Références supplémentaires

Cette référence fournit des liens vers de la documentation et des ressources supplémentaires pour les politiques de prévention des intrusions dans Snort 3 et les informations de cadre MITRE pour la classification des incidents de programmes malveillants.

- [Politique de prévention des intrusions dans Snort 3](#)
- [Modification des politiques de prévention des intrusions Snort 3, à la page 4](#)
- [Informations MITRE dans les incidents de programmes malveillants](#)

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.