Réglage des politiques de prévention des intrusions à l'aide de règles

Les rubriques suivantes expliquent comment utiliser les règles pour ajuster les politiques de prévention des intrusions :

Principes de base du réglage des règles de prévention des intrusions

Vous pouvez utiliser la page Règles dans une politique de prévention des intrusions pour configurer les états des règles et d'autres paramètres pour les règles d'objets partagés, les règles de texte standard et les règles d' de préprocesseur.

Vous activez une règle en définissant son état à Generate Events or to Drop and Generate Events (Générer des événements ou abandonner et générer des événements) (Alerter ou 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 jeu de règles défini sur Drop and Generate Events in an inline deployment (Abandonner et générer des événements dans un déploiement en ligne (blocage) génère des événements et abandonne le trafic correspondant. Dans un déploiement passif, un ensemble de règles sur Drop and Generate Events (Abandonner et générer des événements) génère uniquement des événements sur 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 arguments de règle nécessite un de préprocesseur 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.

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.

Une politique de prévention des intrusions contient :

- *les règles de prévention des intrusions*, qui sont subdivisées en *règles d'objets partagés* et en *règles de texte standard.*
- *les règles de préprocesseur*, qui sont associées à une option de détection du décodeur de paquets ou à l'un des préprocesseurs inclus avec le système

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

Tableau 1 : Règles de prévention des intrusions

Type	ID de générateur (GID)	ID de Snort (SID)	Source	Puis-je copier?	Puis-je effectuer des modifications?
Règle des objets partagés	3	inférieur à 1000000	Talos Intelligence Group	oui	limité
Règle de texte standard	1 (Domaine global ou GID existant)	inférieur à 1000000	Talos	oui	limité
	1000 - 2000 (domaine descendant)	1000000 ou plus	Créé ou importé par l'utilisateur	oui	oui
règle de préprocesseur	propre au décodeur ou au préprocesseur	inférieur à 1000000	Talos	Non	Non
		1000000 ou plus	Généré par le système lors de la configuration des options	Non	Non

Vous ne pouvez pas enregistrer les modifications apportées à 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 aux 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.

Exigences de licence pour les règles de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les politiques de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Affichage des règles d'intrusion dans une politique d'intrusion

Vous pouvez régler l'affichage des règles dans la politique de prévention des intrusions et trier les règles en fonction de plusieurs critères. 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 (contrôle d'accès)** > **Intrusion**.

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

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

Étape 3 Cliquez sur **Rules** (règles) sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Lors de l'affichage des règles, vous pouvez :

- Filtrez les règles comme décrit dans Définition d'un filtre de règles dans une politique de prévention des intrusions, à la page 16.
- Triez les règles en cliquant sur le titre en haut de la colonne selon laquelle vous souhaitez effectuer le tri.
- Afficher les détails d'une règle de prévention des intrusions, comme décrit dans Affichage des détails d'une règle de prévention des intrusions, à la page 6.
- Affichez les règles dans différentes couches de politique en choisissant une couche dans la liste déroulante **Policy** (politiques).

Colonnes de la page des règles de prévention des intrusions

La page des règles de prévention des intrusions utilise les mêmes icônes dans la barre de menus et les en-têtes de colonne. Par exemple, le menu État de la règle utilise la même icône **Generate Events** (Générer des événements) que la colonne État de la règle dans la liste des règles.

Tableau 2 : Colonnes de la page de règles

En-tête	Description
GID	Nombre entier qui indique l'ID de générateur (GID) de la règle.
SID	Entier qui indique le ID de Snort (SID), qui agit comme identifiant unique pour la règle. Pour les règles personnalisées, le SID est 1000000 ou supérieur.
Message	Message inclus dans les événements générés par cette règle, qui sert également de nom de la règle.
Générer des événements	L'état de la règle : • **Supprimer et générer des événements** • **Générer des événements** • **Désactivé** Notez que l'icône d'une règle désactivée est une version grisée de l'icône d'une règle configurée pour générer des événements sans perte de trafic. En outre, si vous cliquez sur l'icône d'état de la règle associée à une règle, vous pouvez modifier l'état de la règle.

En-tête	Description
État de règle recommandé par Cisco	État de règle recommandé par Cisco pour la règle.
Filtre d'événements	Filtre d'événements, y compris les seuils d'événements et la suppression d'événements, appliqué à la règle.
État dynamique	État dynamique de la règle, qui entre en vigueur si des anomalies de débit se produisent.
Erreurs (✖)	Alertes configurées pour la règle (actuellement alertes SNMP uniquement).
Commentaires (💬)	Commentaires ajoutés à la règle.

Vous pouvez également utiliser la liste déroulante des couches pour passer à la page des règles des autres couches de votre politique. Notez que, à moins que vous ajoutiez des couches à votre politique, les seuls affichages modifiables répertoriés dans la liste déroulante sont la page Rules (Règles) de la politique et la page Rules pour une couche de politique initialement nommée `My Changes` (Mes modifications); notez également qu'apporter des modifications dans l'un de ces affichages équivaut à effectuer les modifications dans l'autre. La liste déroulante répertorie également la page Rules pour la politique de base en lecture seule.

Détails des règles de prévention des intrusions

Vous pouvez afficher la documentation sur les règles, les recommandations de Cisco et le surdébit des règles dans la vue Rule Detail (Détail des règles). Vous pouvez également afficher et ajouter des fonctionnalités propres aux règles.

Tableau 3 : Détails de la règle

Article	Description
Résumé	Le résumé de la règle. Pour les événements basés sur des règles, cette ligne s'affiche lorsque la documentation de la règle contient des informations sommaires.
État de la règle	L'état actuel de la règle. Indique également la couche dans laquelle l'état de la règle est défini.
Recommandation de Cisco	Si des recommandations Cisco ont été générées, une icône qui représente l'état de règle recommandé figure; voir Colonnes de la page des règles de prévention des intrusions, à la page 4. Si la recommandation est d'activer la règle, le système indique également les ressources ou les configurations réseau qui ont déclenché la recommandation.
Règle générale	L'impact potentiel de la règle sur les performances du système et la probabilité que la règle génère de faux positifs. Les règles locales n'ont pas de surdébit, sauf si elles sont mappées à une vulnérabilité.
Seuils	les seuils actuellement définis pour cette règle, ainsi que la possibilité d'ajouter un seuil pour la règle.
Suppressions	Les paramètres de suppression actuellement définis pour cette règle, ainsi que la possibilité d'ajouter des suppressions pour la règle.

Article	Description
État dynamique	États des règles basées sur le débit actuellement définis pour cette règle, ainsi que la possibilité d'ajouter des états de règle dynamiques pour la règle.
Alertes	Alertes SNMP définies pour cette règle, ainsi que la possibilité d'ajouter une alerte pour la règle.
Commentaires	Les commentaires ajoutés à cette règle, ainsi que la possibilité d'ajouter des commentaires pour la règle.
Documentation	La documentation de la règle actuelle, fournie par Talos Intelligence Group. Cliquez éventuellement sur **Rule Documentation** (Documentation de la règle) pour afficher des détails plus spécifiques à la règle.

Affichage des détails d'une règle de prévention des intrusions

Procédure

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

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

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

Étape 3 Dans le volet de navigation, cliquez sur **Règles**.

Étape 4 Cliquez sur la règle dont vous souhaitez afficher les détails, puis cliquez sur **Show Details** (Afficher les détails) au bas de la page.
Les détails de la règle s'affichent, comme décrit dans Détails des règles de prévention des intrusions, à la page 5.

Étape 5 À partir des détails de la règle, vous pouvez configurer :

- Alertes : voir Définition d'une alerte SNMP pour une règle de prévention des intrusions, à la page 9.
- Commentaires : Voir Ajout d'un commentaire à une règle de prévention des intrusions, à la page 9.
- États dynamiques des règles : voir Définition d'un état de règle dynamique à partir de la page Rule Details (détails de la règle), à la page 8.
- Seuils : voir Définition d'un seuil pour une règle de prévention des intrusions, à la page 6.
- Suppressions : voir Définition de la suppression pour une règle de prévention des intrusions, à la page 7.

Définition d'un seuil pour une règle de prévention des intrusions

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.

Notez qu'un **Revert** (Revenir en arrière) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add**(Ajouter) à côté de **Thresholds** (Seuils).

Étape 2 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 3 Dans la liste déroulante **Track By** (suivre par), choisissez **Source** ou **Destination** pour indiquer si vous souhaitez que les instances d'événement soient suivies par adresse IP source ou de destination.

Étape 4 Dans le champ **Nombre**, saisissez le nombre d'instances d'événement que vous souhaitez utiliser comme seuil.

Étape 5 Dans le champ **Seconds** (secondes), saisissez un nombre qui spécifie la période, en secondes, pendant laquelle les instances d'événement sont suivies.

Étape 6 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événements** à côté de la règle dans la colonne Event Filtering (filtrage des événements). Si vous ajoutez plusieurs filtres d'événements à une règle, le système inclut une indication du nombre de filtres d'événements.

Définition de la suppression pour une règle de prévention des intrusions

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

Notez qu'un **Revert** (Restaurer) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add** (Ajouter) à côté de **Suppressions**.

Étape 2 Dans la liste déroulante **Suppression type** (Type de suppression), choisissez l'une des options suivantes :

- Choisissez **Rule** (règle) pour supprimer complètement les événements pour une règle sélectionnée.
- Choisissez **Source** pour supprimer les événements générés par les paquets provenant d'une adresse IP source spécifiée.
- Choisissez **Destination** pour supprimer les événements générés par les paquets allant à une adresse IP de destination spécifiée.

Étape 3 Si vous avez choisi **Source** ou **Destination** pour le type de suppression et dans le champ **Network** (réseau), saisissez une adresse IP, un bloc d'adresses ou une liste séparée par des virgules composée de toute combinaison de ces éléments.

Si la politique de prévention des intrusions est associée à l'action par défaut d'une politique de contrôle d'accès, vous pouvez également spécifier ou répertorier une variable de réseau dans l'ensemble des variables d'action par défaut.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 4 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événement** à côté de la règle dans la colonne Event Filtering (filtrage d'événements) à côté de la règle supprimée. Si vous ajoutez plusieurs filtres d'événements à une règle, un numéro au-dessus du filtre indique le nombre de filtres.

Définition d'un état de règle dynamique à partir de la page Rule Details (détails de la règle)

Vous pouvez définir un ou plusieurs états de règle dynamique pour une règle. Le premier état de règle dynamique répertorié a la priorité la plus élevée. Lorsque deux états de règles dynamiques sont en conflit, l'action du premier est effectuée.

Les états des règles dynamiques sont spécifiques à chaque politique.

Notez qu'un **Revert** (Revenir en arrière) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add** (Ajouter) à côté de **Dynamic State** (état dynamique).

Étape 2 Dans la liste déroulante **Track By** (suivre par), choisissez une option pour indiquer comment vous souhaitez que les correspondances de règles soient suivies :

- Choisissez **Source** pour suivre le nombre de résultats pour cette règle à partir d'une source ou d'un ensemble de sources spécifiques.
- Choisissez **Destination** pour suivre le nombre de résultats pour cette règle vers une destination ou un ensemble de destinations spécifiques.
- Choisissez **Rule** (Règle) pour suivre toutes les correspondances pour cette règle.

Étape 3 Si vous définissez **Suivi par source** ou **destination**, saisissez l'adresse IP de chaque hôte que vous souhaitez suivre dans le champ **Network** (Réseau).

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 4 À côté de **Rate**(débit), spécifiez le nombre de correspondances de règles par période pour définir le débit d'attaque :

- Dans le champ **Nombre**, précisez le nombre de correspondances de règles que vous souhaitez utiliser comme seuil.
- Dans le champ **Secondes**, précisez le nombre de secondes qui composent la période pendant laquelle les attaques sont suivies.

Étape 5 Dans la liste déroulante **New State** (Nouvel état), choisissez la nouvelle action à entreprendre lorsque les conditions sont remplies.

Étape 6 Saisissez une valeur dans le champ **Délai d'expiration**.

Une fois l'expiration du délai dépassée, la règle reprend son état d'origine. Saisissez `0` pour éviter que la nouvelle action n'expire.

Étape 7 Cliquez sur **OK**.

Astuces Le système affiche un état dynamique () à côté de la règle dans la colonne Dynamic State (état dynamique). Si vous ajoutez plusieurs filtres d'état de règle dynamique à une règle, un numéro au-dessus des filtres indique le nombre de filtres.

Définition d'une alerte SNMP pour une règle de prévention des intrusions

Vous pouvez définir une alerte SNMP pour une règle à partir de la page Rule Detail (détails de la règle).

Procédure

Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add SNMP Alert** (Ajouter une alerte SNMP) à côté de **Alerts** (Alertes).

Astuces Le système affiche une alerte **Erreurs** () à côté de la règle dans la colonne Alerting (alertes). Si vous ajoutez plusieurs alertes à une règle, le système inclue une indication du nombre d'alertes.

Ajout d'un commentaire à une règle de prévention des intrusions

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add** (Ajouter) à côté de **Comments** (Commentaires).

Étape 2 Dans le champ **Comments** (Commentaires), saisissez un commentaire pour la règle.

Étape 3 Cliquez sur **OK**.

Astuces Le système affiche un **Commentaires** () à côté de la règle dans la colonne Commentaires. Si vous ajoutez plusieurs commentaires à une règle, un numéro au-dessus du commentaire indique le nombre de commentaires.

Étape 4 Pour supprimer un commentaire de règle, cliquez sur **Delete** (Supprimer) dans la section des commentaires de la règle. Vous pouvez uniquement supprimer un commentaire s'il est mis en cache avec des modifications de politique de prévention des intrusions non validées.

Prochaine étape

- Déployer les changements de configuration.

Filtres de règles d'intrusion dans une politique de prévention des intrusions

Vous pouvez filtrer les règles que vous affichez sur la page Rules (règles) en fonction d'un seul critère ou d'une combinaison d'un ou de plusieurs critères.

Les mots-clés Rule Filter (filtre de règles) vous aident à trouver les règles pour lesquelles vous souhaitez appliquer des paramètres de règles, tels que les états de règles ou les filtres d'événements. Vous pouvez filtrer par mot-clé et sélectionner simultanément l'argument du mot-clé en sélectionnant l'argument souhaité dans le panneau de filtre de la page de règles.

Remarques sur les filtres de règles de prévention des intrusions

Le filtre que vous créez est affiché dans la zone de texte Filtrer. Vous pouvez cliquer sur des mots-clés et des arguments de mots-clés dans le panneau des filtres pour créer un filtre. Lorsque vous choisissez plusieurs mots-clés, le système les combine à l'aide de la logique AND pour créer un filtre de recherche composé. Par exemple, si vous choisissez **preprocessor** (Préprocesseur) sous **Category** (Catégorie) puis **Rule Content** > **GID** (Contenu de la règle > GID) et saisissez `116`, vous obtenez un filtre de `Category: "preprocessor" GID:"116"`, qui récupère toutes les règles qui sont des règles de préprocesseurs **et** ont un GID de 116.

Les groupes de filtres Catégorie, Vulnérabilités Microsoft, Vers Microsoft, Propre à la plateforme, Préprocesseur et Priorité vous permettent de soumettre plusieurs arguments pour un même mot-clé, séparés par des virgules. Par exemple, vous pouvez choisir **os-linux** et **os-windows** dans **Catégorie** pour produire la `catégorie de filtre:"os-windows,os-linux"`, qui récupère les règles de la catégorie `os-linux` ou `os-windows`.

Pour afficher le panneau de filtres, cliquez sur l'**icône Afficher**.

Pour masquer le panneau des filtres, cliquez sur l'**icône Masquer**.

Directives de construction des filtres de règles de politique de prévention des intrusions

Dans la plupart des cas, lorsque vous créez un filtre, vous pouvez utiliser le panneau de filtres à gauche de la page des règles dans la politique de prévention des intrusions pour choisir les mots-clés et arguments que vous souhaitez utiliser.

Les filtres de règles sont regroupés en groupes de filtres de règles dans le panneau des filtres. De nombreux groupes de filtres de règles contiennent des sous-critères qui vous permettent de trouver plus facilement les règles spécifiques que vous recherchez. Certains filtres de règles ont plusieurs niveaux que vous pouvez développer pour accéder aux règles individuelles.

Les éléments du panneau de filtres représentent parfois des groupes de types de filtres, parfois des mots-clés et parfois même l'argument d'un mot-clé. Tenez compte des points suivants :

- Lorsque vous choisissez un titre de groupe de type de filtre qui n'est pas un mot-clé (Configuration de la règle, Contenu de la règle, Spécifique à la plate-forme et Priorité), celui-ci se développe pour énumérer les mots-clés disponibles.

  Lorsque vous choisissez un mot-clé en cliquant sur un nœud dans la liste de critères, une fenêtre contextuelle s'affiche, dans laquelle vous devez fournir l'argument selon lequel vous souhaitez filtrer.

  Si ce mot-clé est déjà utilisé dans le filtre, l'argument que vous fournissez remplace l'argument existant pour ce mot-clé.

  Par exemple, si vous cliquez sur **Drop and Generate Events** (Abandonner et générer des événements) sous **Rule Configuration (Configuration de règle)** > **Recommendation (Recommandation)** dans le panneau de filtre, la `recommandation : « Drop and Generate Events »` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **Generate Events** (Générer des événements) sous Rule **Configuration** > **Recommendation** (Recommandation de la configuration de règle), le filtre devient `la recommandation :Generate Events`.

- Lorsque vous choisissez un en-tête de groupe de type de filtre qui est un mot-clé (Catégorie, classifications, vulnérabilités Microsoft, vers Microsoft, priorité et mise à jour des règles), les arguments disponibles sont répertoriés.

  Lorsque vous choisissez un élément dans ce type de groupe, l'argument et le mot-clé auquel il s'applique sont immédiatement ajoutés au filtre. Si le mot-clé est déjà dans le filtre, il remplace l'argument existant du mot-clé qui correspond à ce groupe.

  Par exemple, si vous cliquez sur **os-linux** sous **Catégorie** dans le panneau des filtres, `Category:"os-linux"` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **os-windows** sous **Catégorie**, le filtre devient `Category:"os-windows"`.

- La référence sous le contenu de la règle se trouve dans un mot-clé, tout comme les types d'ID de référence spécifiques répertoriés en dessous de celui-ci. Lorsque vous choisissez l'un des mots-clés de référence, une fenêtre contextuelle s'affiche, dans laquelle vous fournissez un arguments et le mot-clé est ajouté au filtre existant. Si le mot-clé est déjà utilisé dans le filtre, le nouvel arguments que vous fournissez remplace l'argument existant.

  Par exemple, si vous cliquez sur **Rule Content** > **Référence** > **CVE ID** (Contenu de la règle > Référence > CVE ID) dans le panneau de filtre, une fenêtre contextuelle vous invite à fournir l'ID CVE. Si vous saisissez `2007`, `CVE:"2007"` est ajouté à la zone de texte du filtre. Dans un autre exemple, si vous cliquez sur **Rule Content** > **Reference** (Contenu de la règle > Référence) dans le panneau de filtre, une fenêtre contextuelle vous invite à fournir la référence. Si vous saisissez `2007`, la `Reference:"2007"` est ajoutée à la zone de texte du filtre.

- Lorsque vous choisissez des mots-clés de filtre de règles dans différents groupes, chaque mot-clé de filtre est ajouté au filtre et tous les mots-clés existants sont conservés (à moins qu'ils ne soient remplacés par une nouvelle valeur pour le même mot-clé).

  Par exemple, si vous cliquez sur **os-linux** sous **Catégorie** dans le panneau des filtres, `Category:"os-linux"` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **MS00-006** sous **Microsoft Vulnerabilities** (Vulnérabilités Microsoft), le filtre devient `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`.

- Lorsque vous choisissez plusieurs mots-clés, le système les combine à l'aide de la logique AND pour créer un filtre de recherche composé. Par exemple, si vous choisissez **preprocessor** (Préprocesseur) sous **Category** (Catégorie) puis **Rule Content** > **GID** (Contenu de la règle > GID) et saisissez `116`, vous obtenez un filtre de `Category: "preprocessor" GID:"116"`, qui récupère toutes les règles qui sont des règles de préprocesseurs **et** ont un GID de 116.

- Les groupes de filtres Catégorie, Vulnérabilités Microsoft, Vers Microsoft, Propre à la plateforme et Priorité vous permettent de soumettre plusieurs arguments pour un même mot-clé, séparés par des virgules. Par exemple, vous pouvez choisir **os-linux** et **os-windows** dans **Catégorie** pour produire la `catégorie de filtre:"os-windows,app-detect"`, qui récupère les règles de la catégorie `os-linux` ou `os-windows`.

La même règle peut être extraite par plusieurs paires de mots-clés/arguments de filtre. Par exemple, la règle de tentative Cisco DOS (SID 1545) s'affiche si les règles sont filtrées par la catégorie **dos**, mais aussi si vous filtrez selon la priorité **élevée**.

Remarque Talos Intelligence Group peut utiliser le mécanisme de mise à jour des règles pour ajouter et supprimer des filtres de règles.

Notez que les règles de la page Rules (Règles) peuvent être des règles d'objet partagé (générateur ID 3) ou des règles de texte standard (générateur ID 1, domaine global ou GID existant; 1000 à 2000, domaines descendants). Le tableau suivant décrit les différents filtres de règles.

Tableau 4 : Groupes de filtres de règles

Groupe de filtres	Description	Prise en charge d'arguments multiples?	L'en-tête est...	Les éléments de la liste sont...
Configuration de la règle	Recherche des règles en fonction de la configuration de la règle.	Non	Un regroupement	mots-clés
Contenu de la règle	Recherche des règles en fonction de leur contenu.	Non	Un regroupement	mots-clés
Type	Recherche des règles en fonction des catégories de règles utilisées par l'éditeur de règles. Notez que les règles locales s'affichent dans le sous-groupe local.	Oui	Un mot-clé	Arguments
Classifications	Recherche des règles en fonction de la classification de l'attaque qui apparaît dans l'affichage de paquets d'un événement généré par la règle.	Non	Un mot-clé	Arguments
Vulnérabilités de Microsoft	Recherche des règles en fonction du numéro du bulletin Microsoft.	Oui	Un mot-clé	Arguments
Vers de Microsoft	Recherche des règles en fonction de vers spécifiques qui affectent les hôtes Microsoft Windows.	Oui	Un mot-clé	Arguments
Spécifique à la plateforme	Recherche les règles en fonction de leur pertinence pour des versions spécifiques des systèmes d'exploitation. Notez qu'une règle peut affecter plusieurs systèmes d'exploitation ou plusieurs versions d'un système d'exploitation. Par exemple, l'activation de la SID 2260 affecte plusieurs versions de Mac OS X, IBM AIX et autres systèmes d'exploitation.	Oui	Un mot-clé	Arguments Notez que si vous choisissez l'un des éléments de la sous-liste, un modificateur est ajouté à l'argument.

Groupe de filtres	Description	Prise en charge d'arguments multiples?	L'en-tête est...	Les éléments de la liste sont...
Préprocesseurs	Recherche des règles pour des déterminer préprocesseurs individuels. Notez que vous devez activer les règles du préprocesseur associées à une option du préprocesseur générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour celle-ci lorsque le préprocesseur est activé.	Oui	Un regroupement	sous-groupes
Priorité	Recherche des règles en fonction des priorités haute, moyenne et faible. La classification affectée à une règle détermine sa priorité. Ces groupes sont ensuite regroupés en catégories de règles. Notez que les règles locales (c'est-à-dire les règles que vous importez ou créez) n'apparaissent pas dans les groupes de priorité.	Oui	Un mot-clé	Arguments Notez que si vous choisissez l'un des éléments de la sous-liste, un modificateur est ajouté à l'argument.
Mise à jour des règles	Recherche les règles ajoutées ou modifiées par une mise à jour de règle spécifique. Pour chaque mise à jour de règle, affichez toutes les règles de la mise à jour, uniquement les nouvelles règles importées dans la mise à jour ou uniquement les règles existantes modifiées par la mise à jour.	Non	Un mot-clé	Arguments

Filtres de configuration des règles de prévention des intrusions

Vous pouvez filtrer les règles répertoriées dans la page Rules (Règles) en fonction de plusieurs paramètres de configuration de règles. Par exemple, si vous souhaitez afficher l'ensemble de règles dont l'état de règle ne correspond pas à l'état de règle recommandé, vous pouvez filtrer sur l'état de la règle en sélectionnant **Ne correspond pas à la recommandation**.

Lorsque vous choisissez un mot-clé en cliquant sur un nœud de la liste de critères, vous pouvez fournir l'argument selon lequel vous souhaitez filtrer. Si ce mot-clé est déjà utilisé dans le filtre, l'argument que vous fournissez remplace l'argument existant pour ce mot-clé.

Par exemple, si vous cliquez sur **Drop and Generate Events** (Abandonner et générer des événements) sous **Rule Configuration (Configuration de règle)** > **Recommendation (Recommandation)** dans le panneau de filtre, la `recommandation : « Drop and Generate Events »` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **Générer des événements** sous **Configuration des règles** > **Recommandation**, le filtre devient `Recommandation : "Générer des événements"`.

Filtres de contenu de règle de prévention des intrusions

Vous pouvez filtrer les règles répertoriées dans la page Rules (Règles) en fonction de plusieurs éléments de contenu. Par exemple, vous pouvez récupérer rapidement une règle en recherchant le SID de la règle. Vous pouvez également trouver toutes les règles qui inspectent le trafic vers un port de destination spécifique.

Lorsque vous sélectionnez un mot-clé en cliquant sur un nœud de la liste de critères, vous pouvez fournir l'argument selon lequel vous souhaitez filtrer. Si ce mot-clé est déjà utilisé dans le filtre, l'argument que vous fournissez remplace l'argument existant pour ce mot-clé.

Par exemple, si vous cliquez sur **SID** sous **Rule Content** (Contenu de la règle) dans le panneau de filtre, une fenêtre contextuelle s'affiche, vous demandant de fournir un SID. Si vous tapez `1045`, `SID:"1045"`est ajouté à la zone de texte du filtre. Si vous cliquez ensuite sur **SID** à nouveau et modifiez le filtre SID à `1044`, le filtre devient `SID:"1044"`.

Tableau 5 : Filtres de contenu de règle

Ce filtre...	Recherche les règles qui...
Message	contiennent la chaîne fournie dans le champ de message.
SID	ont le SID spécifié.
GID	ont le GID spécifié.
Numéro de référence	contiennent la chaîne fournie dans le champ de référence. Vous pouvez également filtrer par type de référence et par chaîne fournie.
Action	commencent par `alert` ou `pass`.
Protocole	incluent le protocole sélectionné.
Direction	sont basées sur l'inclusion ou non du paramètre directionnel indiqué dans la règle.
IP de la source	utilisent les adresses ou les variables spécifiées pour la désignation de l'adresse IP source dans la règle. Vous pouvez filtrer selon une adresse IP valide, une longueur de bloc ou de préfixe CIDR ou en utilisant des variables telles que `$HOME_NET` ou `$EXTERNAL_NET`.
IP de la destination	utilisent les adresses ou les variables spécifiées pour la désignation de l'adresse IP source dans la règle. Vous pouvez filtrer selon une adresse IP valide, une longueur de bloc ou de préfixe CIDR ou en utilisant des variables telles que `$HOME_NET` ou `$EXTERNAL_NET`.
Port source	incluent le port source spécifié. La valeur du port doit être un entier entre 1 et 65 535 ou une variable de port.
Port de la destination	incluent le port de destination précisé. La valeur du port doit être un entier entre 1 et 65 535 ou une variable de port.
Règle générale	comportentt le surdébit de la règle sélectionnée.
Métadonnées	comportent des métadonnées contenant la paire *clé/valeur* correspondante. Par exemple, saisissez `metadata:"service http"` pour localiser les règles avec des métadonnées relatives au protocole d'application HTTP.

Catégories des règles de prévention des intrusions

Le système Firepower place les règles dans des catégories en fonction du type de trafic détecté par la règle. Dans la page Rules (règles), vous pouvez filtrer par catégorie de règles, afin de pouvoir définir un attribut de

règle pour toutes les règles d'une catégorie. Par exemple, si vous n'avez pas d'hôtes Linux sur votre réseau, vous pouvez filtrer par catégorie **os-linux**, puis désactivez toutes les règles qui s'affichent pour désactiver toute la catégorie **os-linux**.

Vous pouvez passer votre pointeur sur un nom de catégorie pour afficher le nombre de règles de cette catégorie.

Remarque Le Talos Intelligence Group peut utiliser le mécanisme de mise à jour des règles pour ajouter et supprimer des catégories de règles.

Composants du filtre de règles de prévention des intrusions

Vous pouvez modifier votre filtre pour modifier les mots-clés spéciaux et leurs arguments qui sont fournis lorsque vous cliquez sur un filtre dans le panneau des filtres. Les filtres personnalisés de la page de règles fonctionnent comme ceux utilisés dans l'éditeur de règles, mais vous pouvez également utiliser n'importe quel mot-clé fourni dans le filtre de la page de règles, en utilisant la syntaxe affichée lorsque vous sélectionnez le filtre dans le panneau de filtre. Pour déterminer un mot-clé pour une utilisation future, cliquez sur l'argument approprié dans le panneau de filtres à droite. Le mot-clé du filtre et la syntaxe de l'argument s'affichent dans la zone de texte du filtre. Rappelez-vous que plusieurs arguments séparés par des virgules pour un mot-clé ne sont pris en charge que pour les types de filtres Catégorie et Priorité.

Vous pouvez utiliser des mots-clés et des arguments, des chaînes de caractères et des chaînes de caractères littéraux entre guillemets, en séparant plusieurs conditions de filtre. Un filtre ne peut pas inclure d'expressions régulières, de caractères génériques ni d'opérateur spécial tel qu'un caractère de négation (!), un symbole supérieur à (>), inférieur à (|), etc. Lorsque vous saisissez des termes de recherche sans mot-clé, sans majuscule initiale du mot-clé ou sans guillemets autour de l'argument, la recherche est traitée comme une recherche de chaîne et les champs catégorie, message et SID sont recherchés pour les termes spécifiés.

À l'exception des mots-clés `gid` et `sid`, tous les arguments et toutes les chaînes sont traités comme des chaînes partielles. Les arguments pour `gid` et `sid` renvoient uniquement des correspondances exactes.

Chaque filtre de règle peut inclure un ou plusieurs mots-clés au format :

keyword:*"argument"*

où mot-clé est l'un des mots-clés dans les groupes de filtres de la règle de prévention des intrusions et l'argument est mis entre guillemets et correspond à une chaîne alphanumérique unique, insensible à la casse, à rechercher dans le champ ou les champs pertinents pour le mot-clé. Notez que les mots-clés doivent être saisis avec leur majuscule initiale.

Les arguments pour tous les mots-clés, à l'exception de `gid` et `sid`, sont traités comme des chaînes partielles. Par exemple, l'argument `123` renvoie `"12345"`, `"41235"`, `"45123"`, et ainsi de suite. Les arguments de `gid` et `sid` ne renvoient que des correspondances exactes; par exemple, `sid:3080` renvoie uniquement `lSID 3080`.

Chaque filtre de règle peut également inclure une ou plusieurs chaînes de caractères alphanumériques. Les chaînes de caractères recherchent le champ de message de règle, ID de Snort (SID) et l'ID de générateur (GID). Par exemple, la chaîne `123` renvoie les chaînes `"Lotus123"`, `"123Mania"`et ainsi de suite dans le message de règle, et renvoie également `SID 6123`, `SID 12375`, etc. Vous pouvez rechercher un SID partiel en le filtrage avec une ou plusieurs chaînes de caractères.

Toutes les chaînes de caractères sont insensibles à la casse et sont traitées comme des chaînes partielles. Par exemple, les chaînes `ADMIN`, `admin` ou `Admin` renvoient `"admin"`, `"CFADMIN"`, `"Administrator"`, etc.

Vous pouvez mettre des chaînes de caractères entre guillemets pour renvoyer les correspondances exactes. Par exemple, la chaîne littérale `"overflow attempt"` entre guillemets ne renvoie que cette chaîne exacte,

tandis qu'un filtre composé des deux chaînes `overflow` et `attempt` sans guillemets renvoie `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"`, et ainsi de suite.

Vous pouvez affiner les résultats du filtre en saisissant n'importe quelle combinaison de mots-clés, de chaînes de caractères ou des deux, séparés par des espaces. Le résultat inclut toute règle correspondant à toutes les conditions de filtre.

Vous pouvez saisir plusieurs conditions de filtre dans n'importe quel ordre. Par exemple, chacun des filtres suivants renvoie les mêmes règles :

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

Utilisation du filtre de règles de prévention des intrusions

Vous pouvez sélectionner des mots-clés de filtres prédéfinis dans le panneau de filtres sur le côté gauche de la page Rules (Règles) dans la politique de prévention des intrusions. Lorsque vous sélectionnez un filtre, la page affiche toutes les règles correspondantes ou indique lorsqu'aucune règle ne correspond.

Vous pouvez ajouter des mots-clés à un filtre pour le restreindre davantage. Tout filtre que vous saisissez effectue une recherche dans l'ensemble de la base de données des règles et renvoie toutes les règles correspondantes. Lorsque vous saisissez un filtre alors que la page affiche toujours le résultat d'un filtre précédent, la page s'efface et renvoie le résultat du nouveau filtre à la place.

Vous pouvez également saisir un filtre en utilisant le même mot-clé et la même syntaxe d'arguments que ceux fournis lors de la sélection d'un filtre ou modifier les valeurs des arguments dans un filtre après l'avoir sélectionné. Lorsque vous saisissez des termes de recherche sans mot-clé, sans majuscule initiale du mot-clé ou sans guillemets autour de l'argument, la recherche est traitée comme une recherche de chaîne et les champs catégorie, message et SID sont recherchés pour les termes spécifiés.

Définition d'un filtre de règles dans une politique de prévention des intrusions

Vous pouvez filtrer les règles sur la page Rules (Règles) pour afficher un sous-ensemble de règles. Vous pouvez ensuite utiliser n'importe quelle fonctionnalité de la page, y compris en choisissant l'une des fonctionnalités disponibles dans le menu contextuel. Cela peut être utile, par exemple, lorsque vous souhaitez définir un seuil pour toutes les règles d'une catégorie spécifique. Vous pouvez utiliser les mêmes fonctionnalités avec des règles dans une liste filtrée ou non filtrée. Par exemple, vous pouvez appliquer de nouveaux états de règle aux règles d'une liste filtrée ou non.

Tous les mots-clés de filtres, arguments de mots-clés et chaînes de caractères sont insensibles à la casse. Si vous cliquez sur l'argument d'un mot-clé déjà présent dans le filtre, l'argument existant est remplacé.

Procédure

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

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

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

Étape 3 Créez un filtre en utilisant l'une des méthodes suivantes, séparément ou en combinaison :

- Saisissez une valeur dans la zone de texte **Filter** (filtre), puis appuyez sur Entrée.
- Développez l'un des mots-clés prédéfinis. Par exemple, cliquez sur **Rule Configuration**(configuration de la règle).
- Cliquez sur un mot-clé et spécifiez une valeur d'argument si vous y êtes invité. Par exemple :
  - Sous **Rule Configuration**(configuration des règles), vous pouvez cliquer sur **Rule State**(état des règles), choisir `Generate Events` (générer des événements) dans la liste déroulante, puis cliquer sur **OK**.
  - Sous **Rule Configuration**(configuration des règles), vous pouvez cliquer sur **Comment** (commentaires), saisir la chaîne de texte de commentaire à utiliser pour filtrer, puis cliquer sur **OK**.
  - Sous **Category** (Catégorie), vous pouvez cliquer sur **app-detect**, que le système utilise comme valeur d'argument.
- Développez un mot-clé et cliquez sur une valeur d'argument. Par exemple, développez **Rule State** (État de la règle) et cliquez sur **Generate Events** (Générer des évènements).

États des règles d'intrusion

Les états des règles de prévention des intrusions vous permettent d'activer ou de désactiver la règle dans une politique de prévention des intrusions individuelle, ainsi que de spécifier les actions que le système entreprend si des conditions surveillées déclenchent l'application de la règle.

Talos Intelligence Group définit l'état par défaut de chaque règle de prévention des intrusions et de préprocesseur 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'état par défaut d'une ou de plusieurs règles dans une politique par défaut. Si vous permettez aux mises à jour de règles de mettre à jour votre politique de base, vous permettez également à la mise à jour de règle de modifier l'état par défaut d'une règle de votre politique lorsque l'état 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'état de la 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 états par défaut des règles de la politique par défaut que vous utilisez pour créer votre politique.

Options d'état de règle de prévention des intrusions

Dans une politique de prévention des intrusions, vous pouvez définir l'état d'une règle sur les valeurs suivantes :

Générer des événements

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.

Abandonner et générer des événements

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.

Notez que les règles définies pour cet état de règles génèrent des événements mais ne suppriment pas de paquets dans un déploiement passif. Pour que le système abandonne des paquets, l'option **Drop when Inline** (Abandon quand en ligne) doit également être activée (paramètre par défaut) dans votre politique de prévention des intrusions, et vous devez déployer votre périphérique en ligne.

Disable (désactiver)

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

Remarque Choisir l'une des options **Generate Events** (générer des événements) ou **Drop and Generate Events** (abandonner et générer des événements) active la règle. Choisir **Disable** (désactiver) désactive la règle.

Cisco vous recommande **fortement** de **ne pas** activer toutes les règles de prévention des intrusions 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.

Définition des états des règles d'intrusion

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

Procédure

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

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

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

Astuces Cette page indique le nombre total de règles activées, le nombre total de règles activées définies pour générer des événements et le nombre total défini pour supprimer et générer des événements. De plus, dans un déploiement passif, les règles définies pour supprimer et générer des événements servent uniquement à générer des événements.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez définir l'état de la règle.

Étape 5 Effectuez l'une des opérations suivantes :

- **Rule State (état des règles)** > **Generate Events** (générer des événements)
- **Rule State (état des règles)** > **Drop and Generate Events** (supprimer et générer des événements)
- **Rule State (état des règles)** > **Disable** (désactiver)

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, puis cliquez sur **Commit Changes** (valider les modifications).

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

Prochaine étape

- Déployer les changements de configuration.

Filtres de notification d'incident d'intrusion dans une politique d'intrusion

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. Le fait de constater des centaines d'événements identiques ne fait que submerger votre système.

Seuils de incidents d'intrusion

Vous pouvez définir des seuils pour des règles individuelles, par politique de prévention des intrusions, afin de limiter 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. Cela peut vous éviter d'être submergé par un grand nombre d'événements identiques. Vous pouvez définir des seuils par règle d'objet partagé, règle de texte standard ou règle de préprocesseur.

Configuration des seuils d'incidents d'intrusion

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

Tableau 6 : 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.

Option	Description
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 le type sur **Les deux**, **Nombre** sur deux, et **Secondes** sur `10`, il en résulte le décompte des événements suivants : • 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 7 : Options IP de seuil

Option	Description
Source	Calcule le nombre d'instances d'événement par adresse IP source.
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 8 : 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.

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

Sujets connexes

Le mot-clé detection_filter

Ajout et modification de seuils d'incidents d'intrusions

Vous pouvez définir un seuil pour une ou plusieurs règles précises dans une politique de prévention des intrusions. Vous pouvez également modifier séparément ou simultanément les paramètres de seuil existants. Vous ne pouvez définir qu'un seul seuil pour chacune. L'ajout d'un seuil remplace tout seuil existant pour la règle.

Vous pouvez également modifier le seuil global qui s'applique par défaut à toutes les règles et à tous les événements générés par le préprocesseur associés à la politique de prévention des intrusions.

Un **retour arrière** s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Astuces Un seuil global ou individuel sur un périphérique géré avec plusieurs CPU peut entraîner un nombre d'événements plus élevé que prévu.

Procédure

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

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

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

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez définir un seuil.

Étape 5 Choisissez **Event Filtering** > **Threshold**(seuil de filtrage des événements).

Étape 6 Choisissez un type de seuil dans la liste déroulante **Type**.

Étape 7 Dans la liste déroulante **Track By** (suivre par), choisissez si vous souhaitez que les instances d'événement soient suivies par adresse IP **source** ou de **destination**.

Étape 8 Saisissez une valeur dans le champ **Count** (Nombre).

Étape 9 Saisissez une valeur dans le champ **Secondes**.

Étape 10 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événements** à côté de la règle dans la colonne Event Filtering (filtrage des événements). Si vous ajoutez plusieurs filtres d'événements à une règle, un numéro au-dessus du filtre indique le nombre de filtres d'événements.

Étape 11 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

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

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Principes de base des seuils de règle globale

Affichage et suppression des seuils d'incidents d'intrusions

Vous pouvez afficher ou supprimer un paramètre de seuil existant pour une règle. Vous pouvez utiliser la vue Rules Details (détails des règles) pour afficher les paramètres configurés pour un seuil afin de 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.

Notez que vous pouvez également modifier le seuil global qui s'applique par défaut à toutes les règles et à tous les événements générés par le préprocesseur journalisés par la politique de prévention des intrusions.

Procédure

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

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

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

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 4 Choisissez la règle ou les règles avec un seuil configuré que vous souhaitez afficher ou supprimer.

Étape 5 Pour supprimer le seuil de chaque règle sélectionnée, choisissez **Filtrage des événements** > **Supprimer les seuils**.

Étape 6 Cliquez sur **OK**.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

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

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Principes de base des seuils de règle globale

Configuration de la suppression des politiques de prévention des intrusions

Vous pouvez supprimer la notification d'événement d'intrusion dans les cas où une adresse IP spécifique ou une plage d'adresses IP déclenche une règle ou un préprocesseur spécifique. C'est utile pour éliminer les faux positifs. Par exemple, si vous avez un serveur de messagerie qui transmet des paquets qui semblent être une exploitation spécifique, vous pouvez supprimer la notification d'événement pour cet événement 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 le menu contextuel contextuel sur la page de l'éditeur de règles de prévention des intrusions (**Objects (objets)** > **Intrusion Rules (règles d'intrusion)**) et sur n'importe quelle page d'incident d'intrusion (si l'événement a été déclenché par une règle de prévention des intrusions).

Sujets connexes

Le mot-clé detection_filter

Suppression des événements de prévention des intrusions pour une règle spécifique

Vous pouvez supprimer la notification d'incident d'intrusion pour une règle ou des règles dans votre politique de prévention des intrusions. Lorsque la notification est supprimée pour une règle, la règle se déclenche, mais les événements ne sont pas générés. Vous pouvez définir une ou plusieurs suppressions pour une règle. La première suppression répertoriée a la priorité la plus élevée. Lorsque deux suppressions sont en conflit, l'action de la première est effectuée.

Notez qu'un **Revert** (Revenir en arrière) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

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

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

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

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez configurer des conditions de suppression.

Étape 5 Choisissez **Filtrage d'événements** > **Suppression**.

Étape 6 Choisissez un **Type de suppression**

Étape 7 Si vous avez choisi **Source** ou **Destination** pour le type de suppression et que vous souhaitez définir l'adresse IP, le bloc d'adresses ou la variable que vous souhaitez définir comme adresse IP source ou de destination dans le champ **Network** (réseau), saisissez une liste séparée par des virgules de toute combinaison de ces éléments.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 8 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événement** à côté de la règle dans la colonne Event Filtering (filtrage d'événements) à côté de la règle supprimée. Si vous ajoutez plusieurs filtres d'événements à une règle, un numéro au-dessus du filtre indique le nombre de filtres d'événements.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

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

Prochaine étape

- Déployer les changements de configuration.

Affichage et suppression des conditions de suppression

Vous souhaiterez 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 **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

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

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

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez afficher ou supprimer les suppressions.

Étape 5 Vous avez les choix suivants :

- Pour supprimer toutes les suppressions d'une règle, choisissez **Filtrage des événements** > **Supprimer les suppressions**.
- Pour supprimer un paramètre de suppression précis, cliquez sur la règle concernée, puis sur **Show Details** (Afficher les détails). Développez les paramètres de suppression et cliquez sur **Supprimer** à côté des paramètres de suppression que vous souhaitez supprimer.

Étape 6 Cliquez sur **OK**.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

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

Prochaine étape

- Déployer les changements de configuration.

États des règles d'intrusion dynamique

Les attaques basées sur le débit tentent de submerger un réseau ou un hôte en envoyant un trafic excessif vers le réseau ou l'hôte, ce qui entraîne un ralentissement ou le refus de demandes légitimes. Vous pouvez utiliser la prévention basée sur le débit pour modifier l'action d'une règle en réponse au nombre excessif de correspondances de règles pour des règles spécifiques.

Vous pouvez configurer vos politiques de prévention des intrusions pour inclure un filtre basé sur le débit qui détecte lorsqu'un trop grand nombre de correspondances pour une règle se produisent au cours d'une période donnée. Vous pouvez utiliser cette fonctionnalité sur les périphériques gérés déployés en ligne pour bloquer les attaques basées sur le débit pendant une durée spécifiée, puis revenir à un état de règles où les correspondances de règles ne font que générer des événements et ne pas supprimer le trafic.

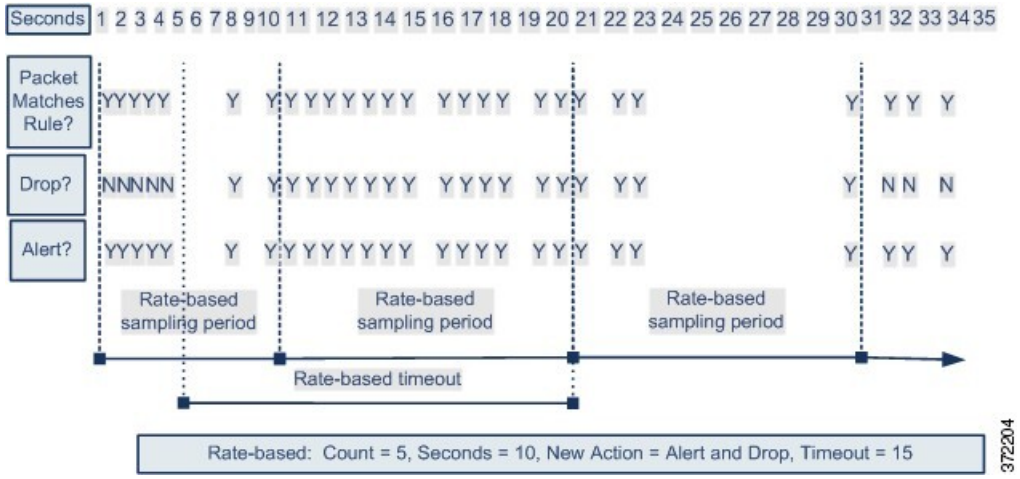
La prévention des attaques basée sur le débit détecte les schémas de trafic anormaux et tente de minimiser l'impact de ce trafic sur les demandes légitimes. Vous pouvez repérer le nombre excessif de correspondances de règles dans le trafic dirigé vers une ou des adresses IP de destination en particulier ou provenant d'une ou

d'adresses IP source en particulier. Vous pouvez également répondre au nombre excessif de correspondances pour une règle particulière dans tout le trafic détecté.

Dans certains cas, vous ne voudrez peut-être pas définir une règle à l'état Abandonner et générer des événements, car vous ne voulez pas supprimer tous les paquets qui correspondent à la règle, mais vous souhaitez supprimer les paquets correspondant à la règle si un taux particulier de correspondances se produit dans un délai déterminé. Les états de règles dynamiques vous permettent de configurer le débit qui doit déclencher une modification de l'action pour une règle, ce que l'action doit changer lorsque le débit est atteint et combien de temps la nouvelle action doit persister.

Le diagramme suivant montre un exemple dans lequel un agresseur tente d'accéder à un hôte. Les tentatives répétées pour trouver un mot de passe déclenchent une règle pour laquelle la prévention des attaques basée sur le débit est configurée. Les paramètres basés sur le débit remplacent l'attribut de règle par Abandon et génération d'événements après cinq correspondances de règles en 10 secondes. Le nouvel attribut de règle expire après 15 secondes.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si le débit échantillonné est supérieur au seuil au cours de la période d'échantillonnage en cours ou précédente, la nouvelle action se poursuit. La nouvelle action ne revient à Générer des événements qu'à la fin d'une période d'échantillonnage au cours de laquelle la fréquence échantillonnée était inférieure à la fréquence seuil.



Configuration de l'état de la règle de prévention des intrusions dynamique

Dans la politique de prévention des intrusions, vous pouvez configurer un filtre basé sur le débit pour toute règle de prévention des intrusions ou de préprocesseur. Le filtre basé sur le débit contient trois composants :

- le taux de correspondance des règles, que vous configurez comme nombre de correspondances de règles dans un nombre spécifique de secondes
- nouvelle action à entreprendre lorsque le débit est dépassé. Trois actions sont possibles: Générer des événements, Supprimer et Générer des événements, et Désactiver
- la durée de l'action, que vous configurez comme valeur de délai d'expiration

Notez qu'une fois démarrée, la nouvelle action se produit jusqu'à ce que le délai soit atteint, même si le débit tombe en dessous du débit configuré pendant cette période. Lorsque le délai d'expiration est atteint, si le débit est inférieur au seuil, l'action effectuée pour la règle reprend l'action initialement configurée pour la règle.

Vous pouvez configurer la prévention des attaques basée sur le débit dans un déploiement en ligne pour bloquer les attaques, de façon temporaire ou permanente. Sans configuration basée sur le débit, les règles définies sur Generate Events génèrent des événements, mais le système ne supprime pas de paquets pour ces règles. Cependant, si le trafic d'attaque correspond aux règles qui ont des critères basés sur le débit configurés, l'action de débit peut entraîner l'abandon de paquets pendant la période pendant laquelle l'action de débit est active, même si ces règles ne sont pas initialement définies sur Abandon et Generate Events .

Remarque Les actions basées sur le débit ne peuvent pas activer les règles désactivées ni abandonner le trafic correspondant aux règles désactivées.

Vous pouvez définir plusieurs filtres basés sur le débit sur la même règle. Le premier filtre répertorié dans la politique de prévention des intrusions a la priorité la plus élevée. Notez que lorsque deux actions de filtres basés sur le débit entrent en conflit, l'action du premier filtre basé sur le débit est exécutée.

Définition d'un état de règle dynamique à partir de la page Rules (Règles)

Vous pouvez définir un ou plusieurs états de règle dynamique pour une règle. Le premier état de règle dynamique répertorié a la priorité la plus élevée. Lorsque deux états de règles dynamiques sont en conflit, l'action du premier est effectuée.

Les états des règles dynamiques sont spécifiques à chaque politique.

Un **retour arrière** s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Remarque Les états de règles dynamiques ne peuvent pas activer les règles désactivées ou abandonner le trafic qui correspond aux règles désactivées.

Procédure

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

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

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

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 4 Sélectionnez la ou les règles pour lesquelles vous souhaitez ajouter un état de règle dynamique.

Étape 5 Choisissez **État dynamique** > **Ajouter un état de règle basé sur le débit**.

Étape 6 Choisissez une valeur dans la liste déroulante **Suivre par**.

Étape 7 Si vous définissez **Suivi par** à **source** ou à **destination**, saisissez l'adresse de chaque hôte que vous souhaitez suivre dans le champ **Network** (Réseau). Vous pouvez spécifier une adresse IP unique, un bloc d'adresses, une variable ou une liste séparée par des virgules composée de n'importe quelle combinaison de ces éléments.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 8 À côté de **Rate**(débit), spécifiez le nombre de correspondances de règles par période pour définir le débit d'attaque :

- Saisissez une valeur dans le champ **Count** (Nombre).
- Saisissez une valeur dans le champ **Secondes**.

Étape 9 Dans la liste déroulante **New State** (Nouvel état), précisez la nouvelle action à entreprendre lorsque les conditions sont remplies.

Étape 10 Saisissez une valeur dans le champ **Délai d'expiration**.

Une fois l'expiration du délai dépassée, la règle reprend son état d'origine. Précisez `0` ou laissez le champ **Délai d'expiration** vide pour empêcher la nouvelle action d'expirer.

Étape 11 Cliquez sur **OK**.

Astuces Le système affiche un **état dynamique** à côté de la règle dans la colonne Dynamic State (état dynamique). Si vous ajoutez plusieurs filtres d'état de règle dynamique à une règle, un numéro au-dessus du filtre indique le nombre de filtres.

Astuces Pour supprimer tous les paramètres de règles dynamiques pour un ensemble de règles, sélectionnez les règles dans la page des règles , puis sélectionnez **État dynamique** > **Supprimer les états basés sur les débits**. Vous pouvez également supprimer des filtres d'état de règle basés sur le débit des détails de la règle en sélectionnant la règle, en cliquant sur **Afficher les détails**, puis en cliquant sur **Supprimer** à côté du filtre basé sur le débit que vous souhaitez supprimer.

Étape 12 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

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

Prochaine étape

- Déployer les changements de configuration.

Ajout de commentaires à la règle de prévention des intrusions

Vous pouvez ajouter des commentaires aux règles de votre politique de prévention des intrusions. Les commentaires ajoutés de cette façon sont propres à la politique; c'est-à-dire que 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. Tous les commentaires que vous ajoutez s'affichent dans la vue Rule Details (détails de la règle) dans la page Rules (Règles) de la politique de prévention des intrusions.

Après avoir validé les modifications de la politique de prévention des intrusions contenant le commentaire, vous pouvez également afficher le commentaire en cliquant sur **Rule Comment** (Commentaire de règle) dans la page de modification de la règle.

Procédure

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

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

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

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez ajouter un commentaire.

Étape 5 Choisissez **Comments** > **Add Rule Comment** (ajouter un commentaire de règle).

Étape 6 Dans le champ **Comments** (Commentaires), saisissez un commentaire pour la règle.

Étape 7 Cliquez sur **OK**.

Astuces Le système affiche un **Commentaires** ( ) à côté de la règle dans la colonne Commentaires. Si vous ajoutez plusieurs commentaires à une règle, un numéro au-dessus du commentaire indique le nombre de commentaires.

Étape 8 Vous pouvez également supprimer un commentaire de règle en cliquant sur **Delete** (Supprimer) à côté du commentaire.

Vous pouvez uniquement supprimer un commentaire s'il est mis en cache avec des modifications de politique de prévention des intrusions non validées. Une fois les modifications apportées à la politique de prévention des intrusions validées, le commentaire de règle est permanent.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

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

Prochaine étape

- Déployer les changements de configuration.

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.