Configurer la stratégie d'intrusion et la configuration des signatures dans le module Firepower (gestion intégrée)

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Informations générales
Configuration
Étape 1. Configurer la stratégie d'intrusion
Étape 1.1. Créer une stratégie d'intrusion
Étape 1.2. Modifier la stratégie d'intrusion
Étape 1.3. Modifier la stratégie de base
Étape 1.4. Filtrage des signatures avec option de barre de filtre
Étape 1.5. Configurer l'état de la règle
Étape 1.6. Configuration du filtre d'événements
Étape 1.7. Configurer l'état dynamique
Étape 2. Configurer la stratégie d'analyse réseau (NAP) et les jeux de variables (facultatif)
Étape 3 : Configurer le contrôle d'accès pour inclure la stratégie d'intrusion/les jeux de variables NAP/NAP
Étape 4. Déployer la stratégie de contrôle d'accès
Étape 5. Surveiller les événements d'intrusion
Vérification
Dépannage
Informations connexes

Introduction

Ce document décrit la fonctionnalité IPS (Intrusion Prevention System)/IDS (Intrusion Detection System) du module FirePOWER et divers éléments de la politique d'intrusion qui établissent une politique de détection dans le module FirePOWER.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

* Connaissance du pare-feu ASA (Adaptive Security Appliance), de l'Adaptive Security Device Manager (ASDM).

* Connaissances FirePOWER Appliance.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Modules ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) exécutant les versions 5.4.1 et ultérieures du logiciel.

Module ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) exécutant les versions 6.0.0 et ultérieures du logiciel.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

FirePOWER IDS/IPS est conçu pour examiner le trafic réseau et identifier les modèles (ou signatures) malveillants qui indiquent une attaque réseau/système. Le module FirePOWER fonctionne en mode IDS si la stratégie de service de l'ASA est spécifiquement configurée en mode moniteur (proche), sinon il fonctionne en mode en ligne.

FirePOWER IPS/IDS est une approche de détection basée sur les signatures. FirePOWERmodule en mode IDS génère une alerte lorsque la signature correspond au trafic malveillant, tandis que FirePOWER en mode IPS génère une alerte et bloque le trafic malveillant.

> **Remarque**:: Assurez-vous que le module FirePOWER doit avoir une licence **Protect** pour configurer cette fonctionnalité. Pour vérifier la licence, accédez à **Configuration > ASA FirePOWER Configuration > License.**

Configuration

Étape 1. Configurer la stratégie d'intrusion

Étape 1.1. Créer une stratégie d'intrusion

Pour configurer la stratégie d'intrusion, connectez-vous à Adaptive Security Device Manager (ASDM) et complétez ces étapes :

Étape 1. Accédez à **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy**.

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

Étape 3. Entrez le **nom** de la stratégie d'intrusion.

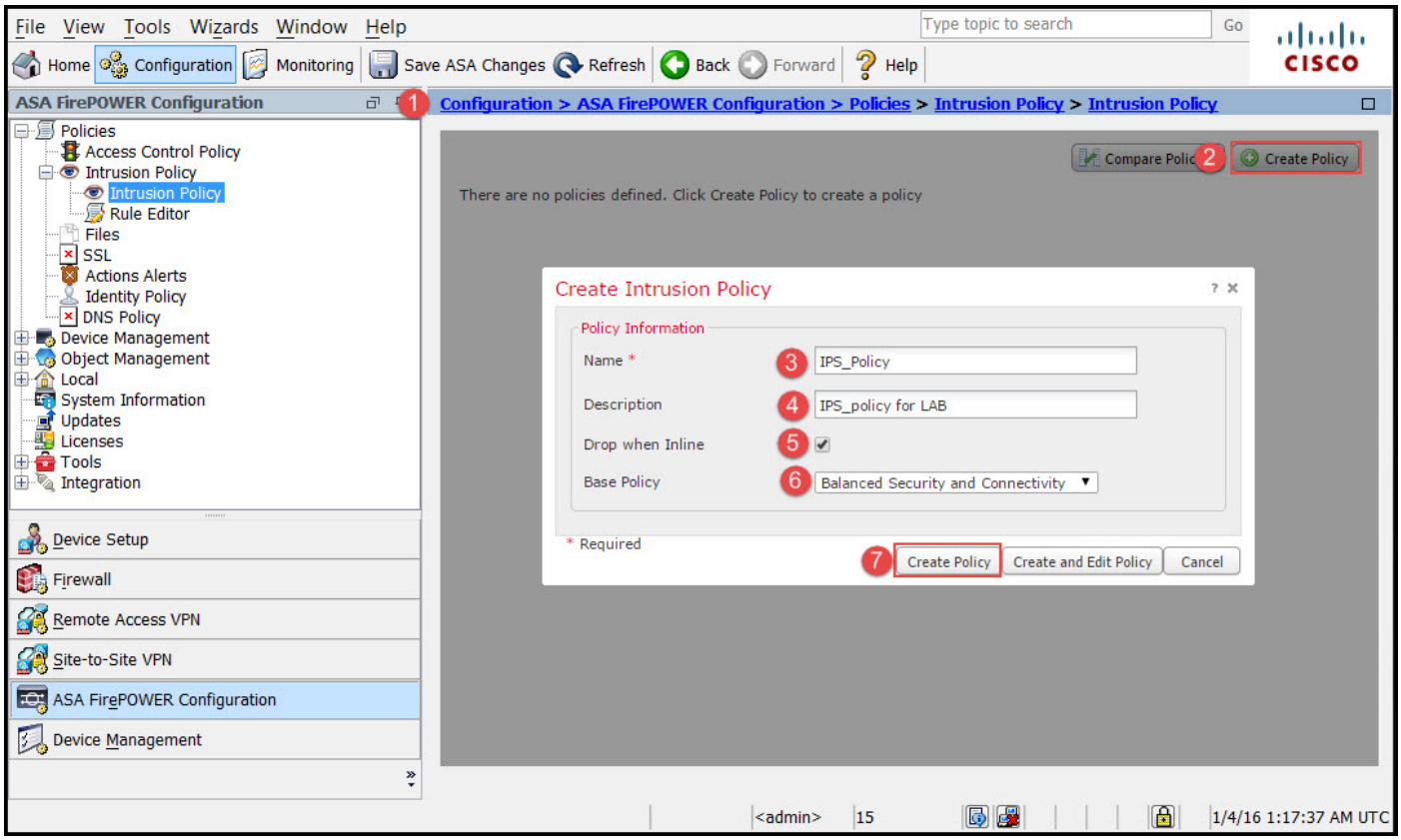
Étape 4. Entrez la **description** de la stratégie d'intrusion (facultatif).

Étape 5. Spécifiez l'option **Déposer en ligne**.

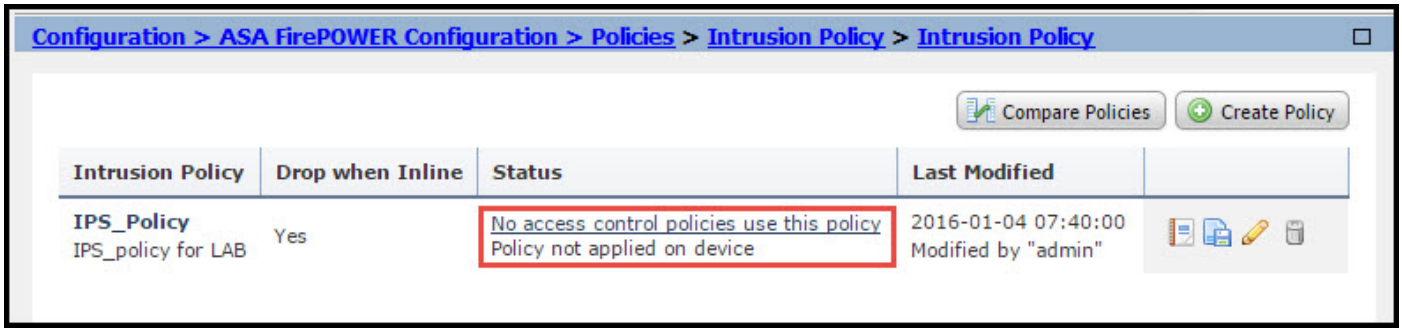
Étape 6. Sélectionnez la **stratégie de base** dans la liste déroulante.

Étape 7. Cliquez sur **Créer une stratégie** pour terminer la création d'une stratégie d'intrusion.

> **Conseil** : Abandonner lorsque l'option Inline est cruciale dans certains scénarios lorsque le capteur est configuré en mode Inline et qu'il est nécessaire de ne pas abandonner le trafic même s'il correspond à une signature qui a une action Drop.

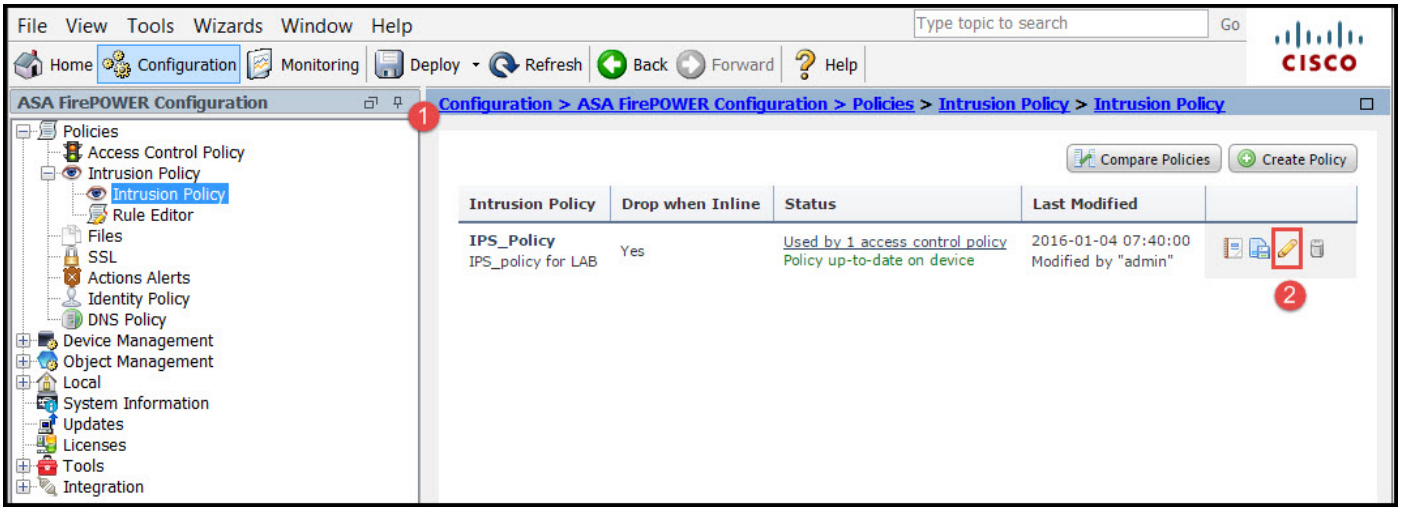


Vous pouvez remarquer que la stratégie est configurée, mais qu'elle n'est appliquée à aucun périphérique.



Étape 1.2. Modifier la stratégie d'intrusion

Pour modifier la stratégie d'intrusion, accédez à **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy** et sélectionnez **Edit** option.

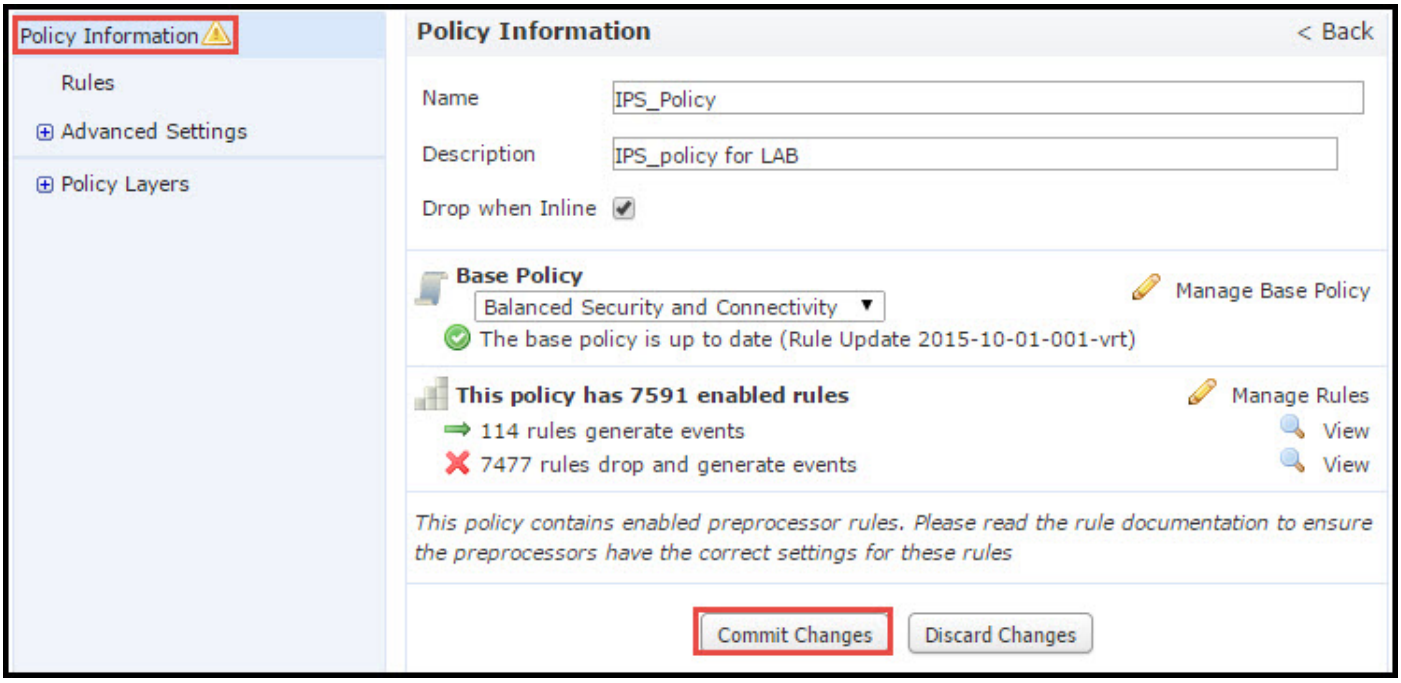


Étape 1.3. Modifier la stratégie de base

La page Intrusion Policy Management permet de modifier l'option Base Policy/Drop lorsque Inline/ Save and Discard.

La stratégie de base contient certaines stratégies fournies par le système, qui sont des stratégies intégrées.

1. Sécurité et connectivité équilibrées : il s'agit d'une politique optimale en termes de sécurité et de connectivité. Cette stratégie a environ 7500 règles activées, certaines d'entre elles génèrent uniquement des événements tandis que d'autres génèrent des événements et abandonnent le trafic.
2. Sécurité plutôt que connectivité :Si vous préférez la sécurité, vous pouvez choisir la sécurité plutôt que la stratégie de connectivité, ce qui augmente le nombre de règles activées.
3. Connectivité plutôt que sécurité : si votre préférence est la connectivité plutôt que la sécurité, vous pouvez choisir la connectivité plutôt que la stratégie de sécurité, ce qui réduira le nombre de règles activées.
4. Maximum Detection (Détection maximale) : sélectionnez cette stratégie pour obtenir une détection maximale.
5. Aucune règle active : cette option désactive toutes les règles. Vous devez activer les règles manuellement en fonction de votre stratégie de sécurité.



Étape 1.4. Filtrage des signatures avec option de barre de filtre

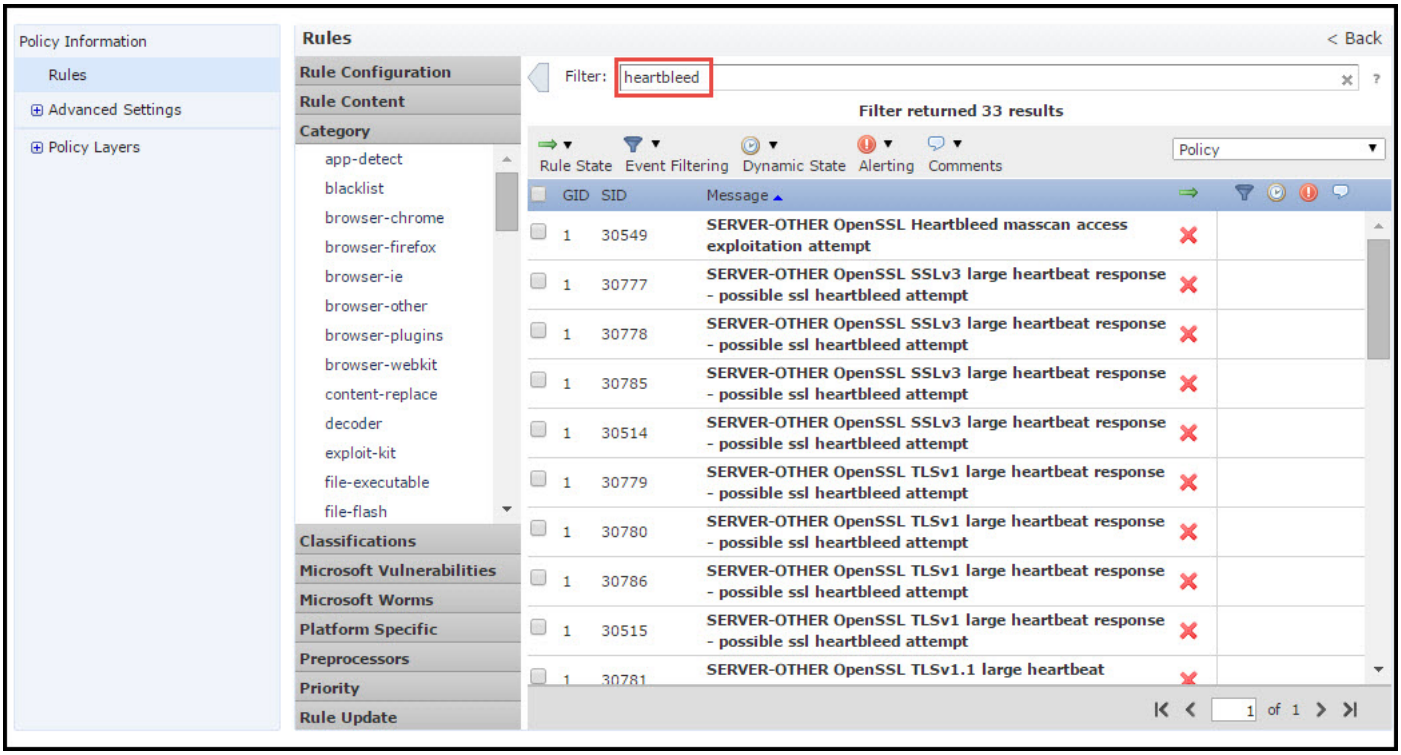
Accédez à l'option **Règles** du panneau de navigation et la page Gestion des règles s'affiche. Il y a des milliers de règles dans la base de données des règles. La barre de filtre offre une bonne option de moteur de recherche pour effectuer une recherche efficace de la règle.

Vous pouvez insérer n'importe quel mot clé dans la barre de filtre et le système saisit les résultats pour vous. S'il est nécessaire de trouver la signature pour la vulnérabilité de type « heartbleed » SSL (Secure Sockets Layer), vous pouvez rechercher mot clé heartbleed dans la barre de filtre et il récupérera la signature pour la vulnérabilité de type « heartbleed ».

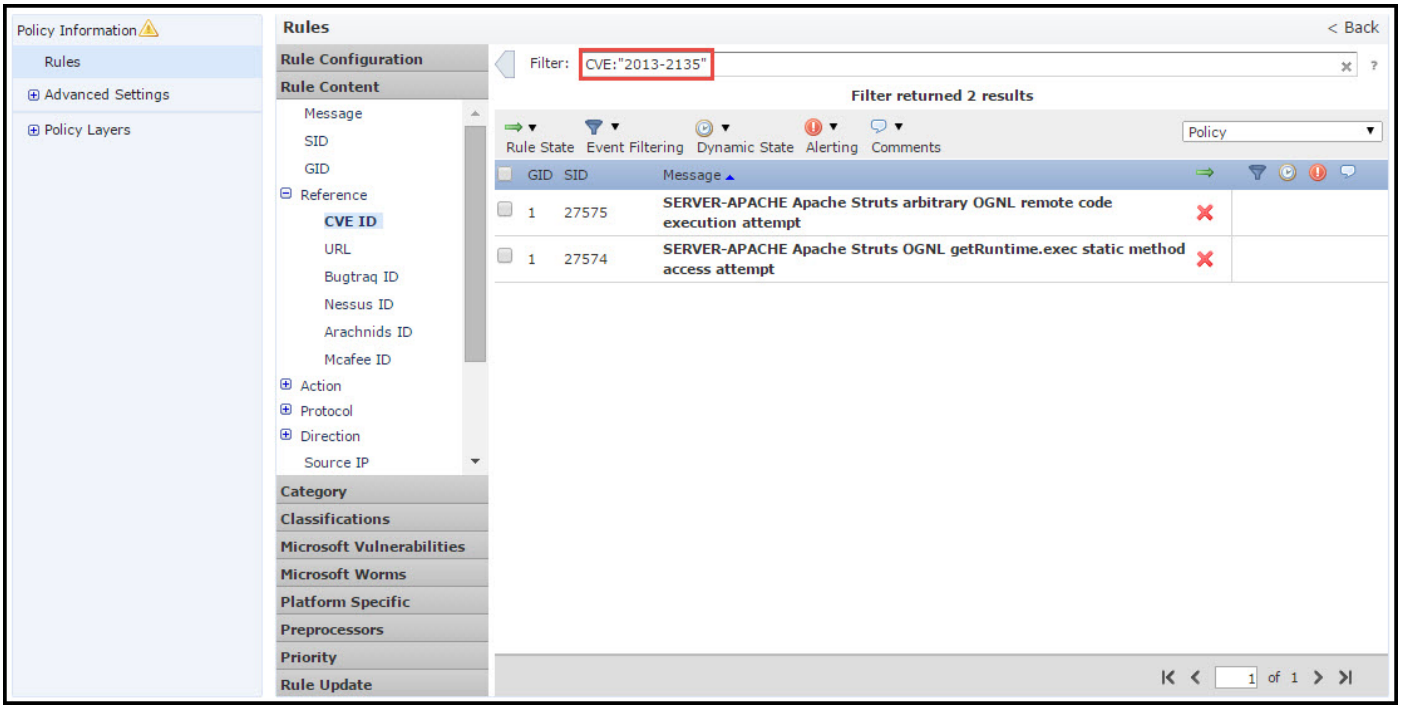
> **Conseil** : si plusieurs mots clés sont utilisés dans la barre de filtre, le système les combine en utilisant la logique AND pour créer une recherche composée.

Vous pouvez également rechercher les règles à l'aide de l'ID de signature (SID), de l'ID de générateur (GID), de la catégorie : à faire, etc.

Les règles sont effectivement divisées en plusieurs façons, par exemple en fonction des catégories/classifications/vulnérabilités Microsoft/vers Microsoft/ spécifiques à la plate-forme. Une telle association de règles permet au client d'obtenir facilement la bonne signature et d'aider le client à régler efficacement les signatures.



Vous pouvez également rechercher avec le numéro CVE pour trouver les règles qui les couvrent. Vous pouvez utiliser la syntaxe **CVE : <cve-number>.**



Étape 1.5. Configurer l'état de la règle

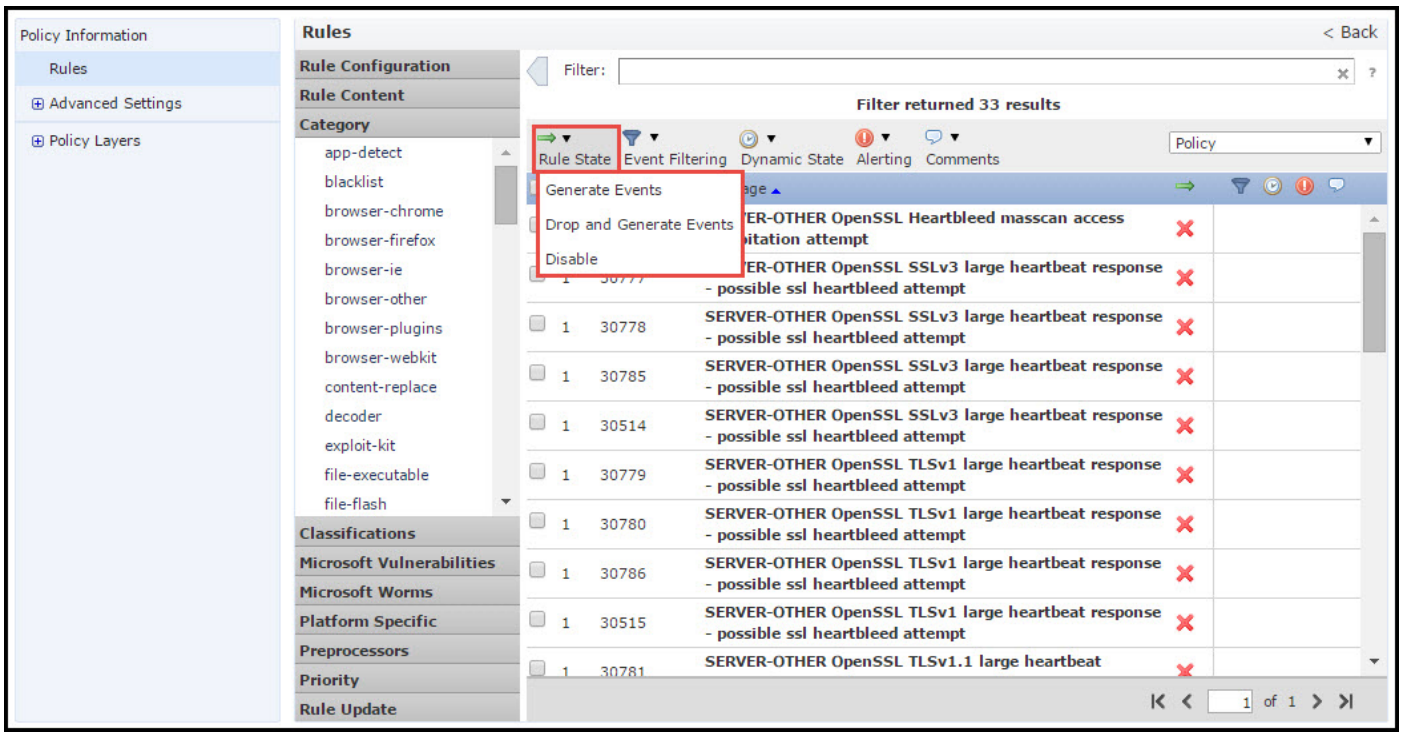
Accéder à **Règles** dans le panneau de navigation et la page Gestion des règles s'affiche. Sélectionnez les règles et choisissez l'option **État de la règle** pour configurer l'état des règles. Il existe trois états qui peuvent être configurés pour une règle :

1. **Générer des événements :** Cette option génère des événements lorsque la règle correspond au trafic.

2. **Drop and Generate Events :** cette option génère des événements et supprime le trafic lorsque

la règle correspond au trafic.

3. **Désactiver :** Cette option désactive la règle.



Étape 1.6. Configuration du filtre d'événements

L'importance d'un événement d'intrusion peut être basée sur la fréquence d'occurrence, ou sur l'adresse IP source ou de destination. Dans certains cas, vous pouvez ne pas vous soucier d'un événement avant qu'il ne se soit produit un certain nombre de fois. Par exemple, vous pouvez ne pas être inquiet si quelqu'un tente de se connecter à un serveur jusqu'à ce qu'il échoue un certain nombre de fois. Dans d'autres cas, vous n'aurez peut-être besoin de voir que quelques occurrences de règle frappées pour vérifier s'il y a un problème généralisé.

Il existe deux façons d'y parvenir :

1. Seuil d'événements.

2. Suppression des événements.

Seuil d'événement

Vous pouvez définir des seuils qui déterminent la fréquence d'affichage d'un événement, en fonction du nombre d'occurrences. Vous pouvez configurer le seuil par événement et par stratégie.

Étapes de configuration du seuil d'événement :

Étape 1. Sélectionnez la **ou les règles** pour lesquelles vous souhaitez configurer le seuil d'événement.

Étape 2. Cliquez sur le **filtrage des événements**.

Étape 3. Cliquez sur le **seuil**.

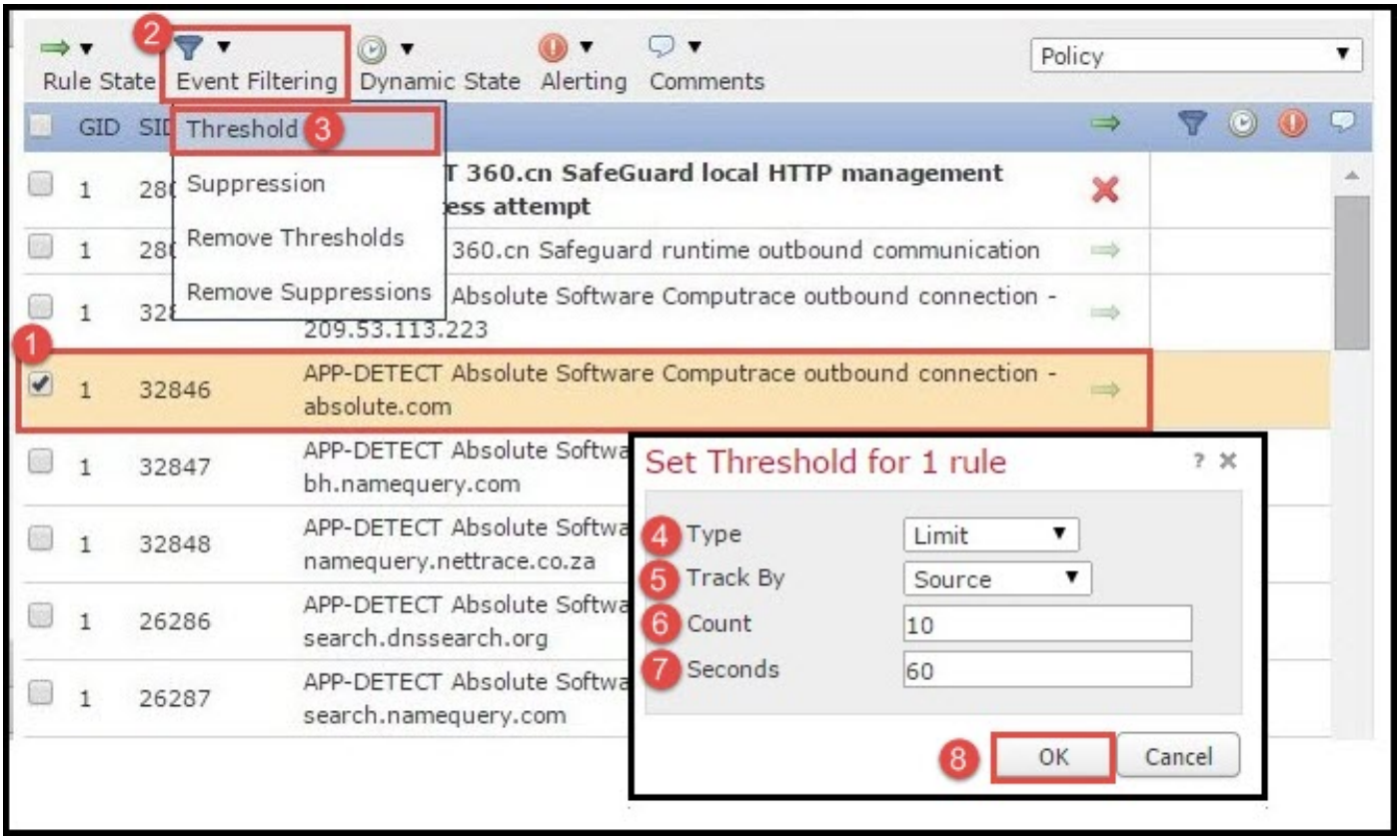
Étape 4. Sélectionnez le **type** dans la liste déroulante. (Limite ou Seuil ou Les deux).

Étape 5. Sélectionnez le mode de suivi dans la zone de liste déroulante **Suivi par**. (Source ou Destination).

Étape 6. Entrez le **nombre** d'événements à atteindre.

Étape 7. Entrez les **secondes** à écouler avant la réinitialisation du nombre.

Étape 8. Cliquez sur **OK pour terminer.**



Après l'ajout d'un filtre d'événement à une règle, vous devriez voir une icône de filtre en regard de l'indication de règle, qui indique qu'un filtrage d'événement est activé pour cette règle.

Suppression d'événements

Les notifications d'événements spécifiés peuvent être supprimées en fonction de l'adresse IP source/de destination ou par règle.

Note: Lorsque vous ajoutez la suppression d'événements pour une règle. L'inspection des signatures fonctionne normalement, mais le système ne génère pas les événements si le trafic correspond à la signature. Si vous spécifiez une source/destination spécifique, les événements n'apparaissent pas uniquement pour la source/destination spécifique de cette règle. Si vous choisissez de supprimer la règle complète, le système ne génère aucun événement pour cette règle.

Étapes de configuration du seuil d'événement :

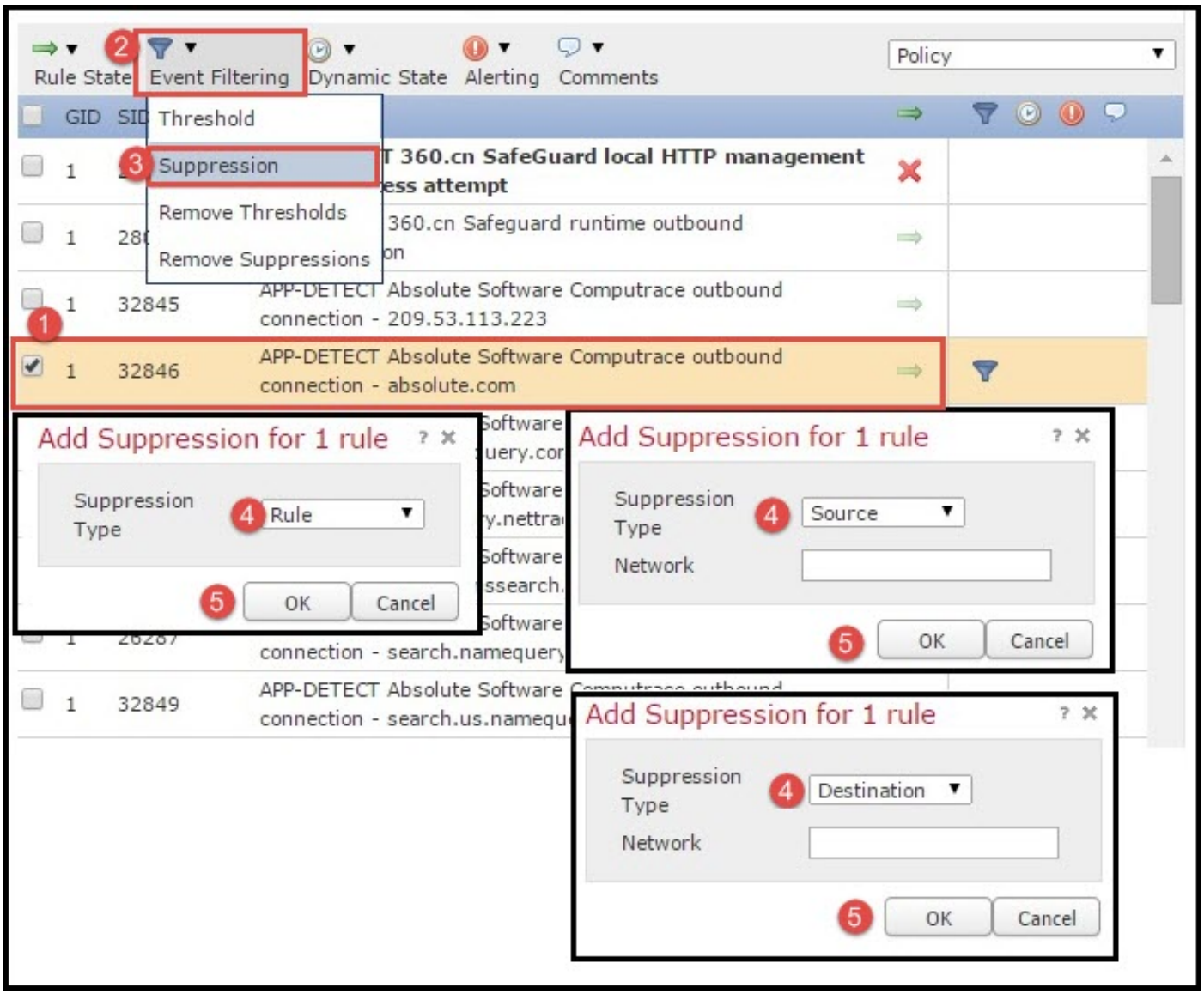
Étape 1. Sélectionnez la **ou les règles** pour lesquelles vous souhaitez configurer le seuil d'événement.

Étape 2. Cliquez sur **Filtrage des événements**.

Étape 3. Cliquez sur **Suppression.**

Étape 4. Sélectionnez **Type de suppression** dans la liste déroulante. (Règle ou Source ou Destination).

Étape 5. Cliquez sur **OK pour terminer.**



Une fois le filtre d'événement ajouté à cette règle, vous devriez voir une icône de filtre avec le nombre deux en regard de l'indication de règle, qui indique que deux filtres d'événement sont activés pour cette règle.

Étape 1.7. Configurer l'état dynamique

Il s'agit d'une fonction dans laquelle nous pouvons modifier l'état d'une règle si la condition spécifiée correspond.

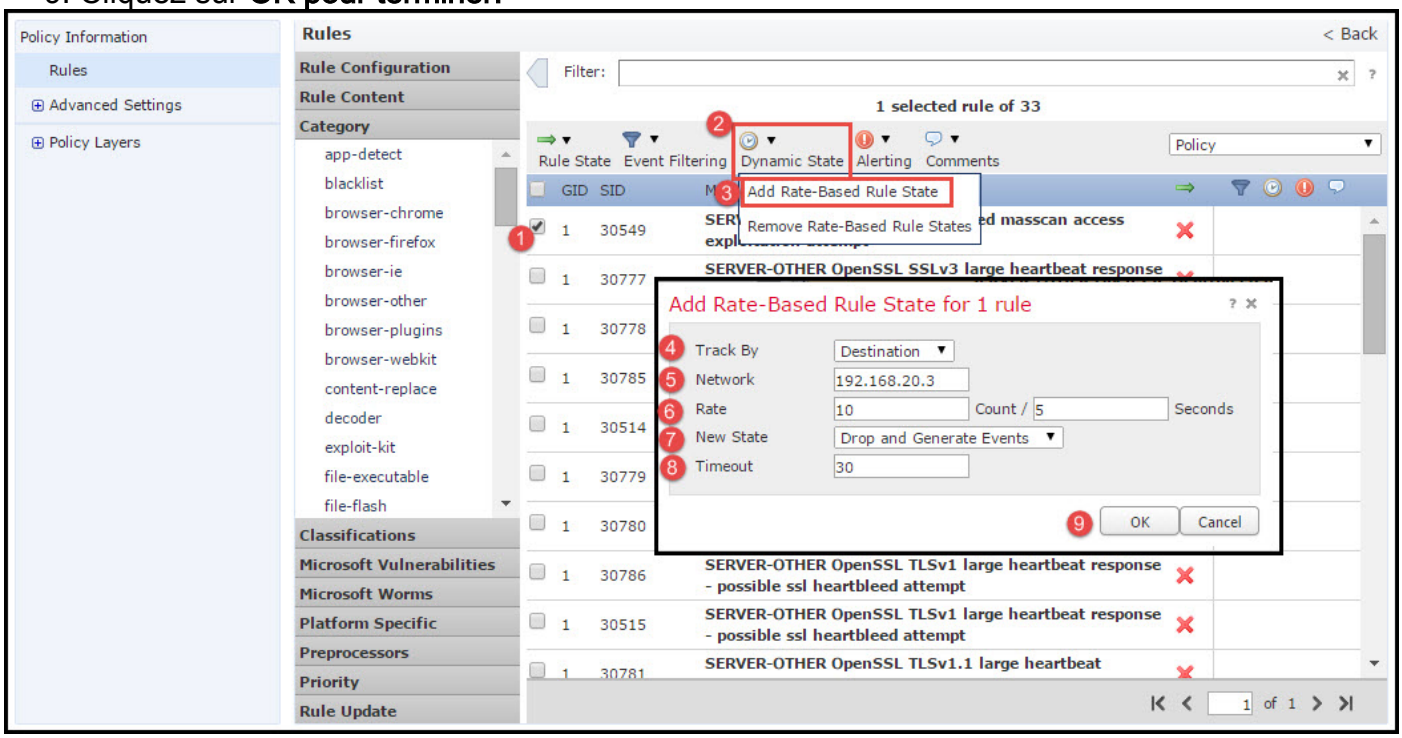
Supposons qu'un scénario d'attaque en force frappe le mot de passe. Si une signature détecte une tentative d'échec du mot de passe et que l'action de la règle consiste à générer un événement. Le système continue à générer l'alerte pour la tentative d'échec du mot de passe. Dans ce cas, vous pouvez utiliser l'**état dynamique** où une action de **Générer des événements**

peut être modifiée pour **Supprimer et générer des événements** pour bloquer l'attaque de force brute.

Accéder à **Règles** dans le panneau de navigation et la page Gestion des règles s'affiche. Sélectionnez la règle pour laquelle vous voulez activer l'état dynamique et choisissez les options **État dynamique > Ajouter un état de règle de base de taux.**

Pour configurer l'état de la règle basée sur le débit :

1. Sélectionnez la **ou les règles** pour lesquelles vous souhaitez configurer le seuil d'événement.
2. Cliquez sur l'**état dynamique**.
3. Cliquez sur l'**état Add Rate-Based Rule**.
4. Sélectionnez le mode de suivi de l'état de la règle dans la zone de liste déroulante **Suivi par**. (**Règle ou Source ou Destination**).
5. Saisissez le **réseau**. Vous pouvez spécifier une adresse IP, un bloc d'adresses, une variable ou une liste séparée par des virgules, qui comprend n'importe quelle combinaison de ces éléments.
6. Entrez le **nombre** d'événements et l'horodatage en secondes.
7. Sélectionnez le **nouvel état,** que vous voulez définir pour la règle.
8. Entrez le **délai d'attente** après lequel l'état de la règle est rétabli.
9. Cliquez sur **OK pour terminer.**



Étape 2. Configurer la stratégie d'analyse réseau (NAP) et les jeux de variables (facultatif)

Configurer la stratégie d'analyse réseau

La stratégie d'accès au réseau est également appelée préprocesseurs. Le préprocesseur réassemble les paquets et normalise le trafic. Il permet d'identifier les anomalies de protocole de couche réseau et de couche transport lors de l'identification d'options d'en-tête inappropriées.

NAP effectue la défragmentation des datagrammes IP, assure l'inspection dynamique TCP et le

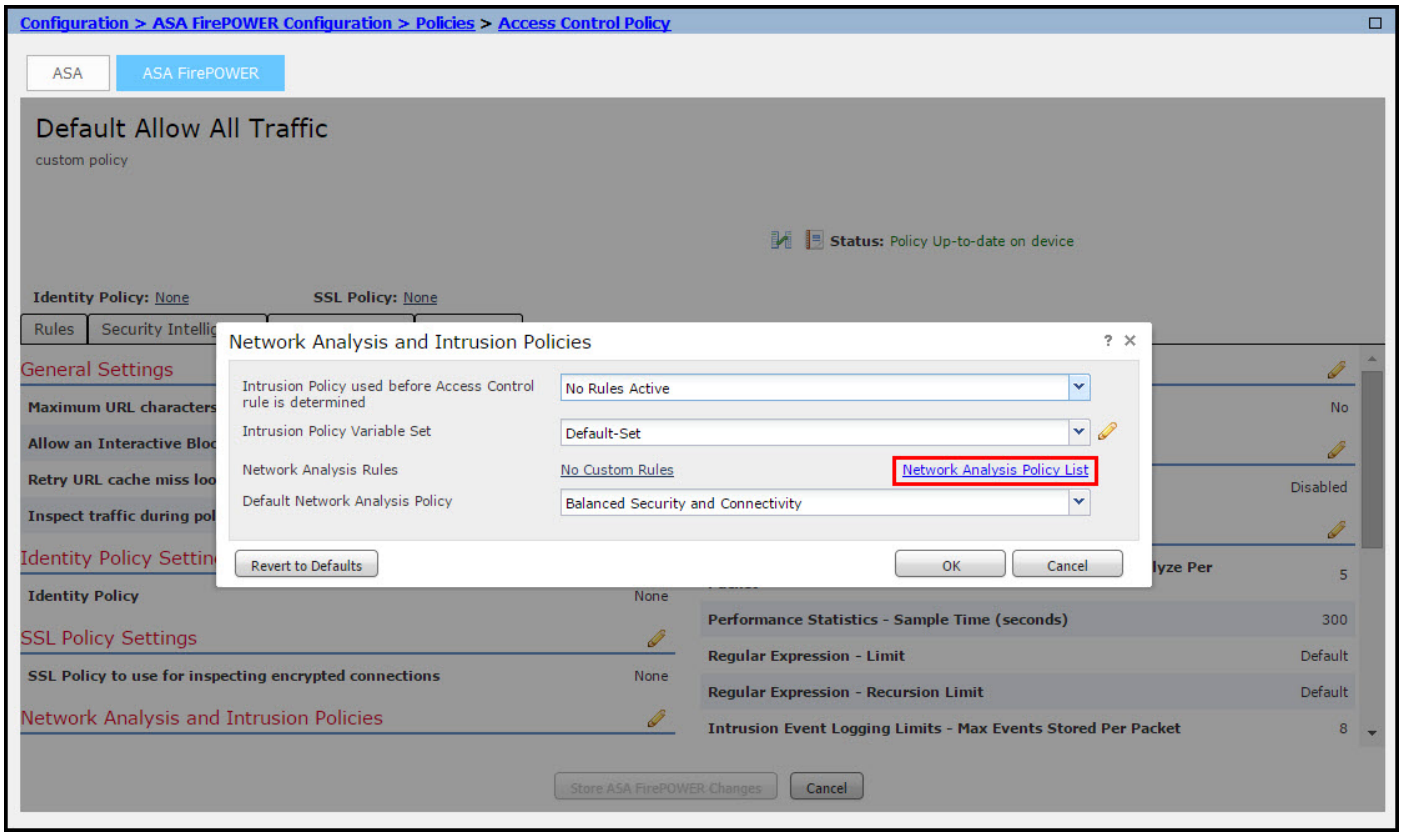
réassemblage des flux, ainsi que la validation des sommes de contrôle. Le préprocesseur normalise le trafic, valide et vérifie la norme de protocole.

Chaque préprocesseur a son propre numéro GID. Il représente le préprocesseur qui a été déclenché par le paquet.

Pour configurer la stratégie d'analyse du réseau, accédez à **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy > Advanced > Network Analysis and Intrusion Policy.**

La stratégie d'analyse du réseau par défaut est Sécurité et connectivité équilibrées, qui est la stratégie recommandée optimale. Il existe trois autres politiques NAP fournies par le système qui peuvent être sélectionnées dans la liste déroulante.

Sélectionnez l'option **Network Analysis Policy** List pour créer une stratégie NAP personnalisée.



Configurer les jeux de variables

Les jeux de variables sont utilisés dans les règles d'intrusion pour identifier les adresses et les ports source et de destination. Les règles sont plus efficaces lorsque les variables reflètent plus fidèlement votre environnement réseau. La variable joue un rôle important dans le réglage des performances.

Les jeux de variables ont déjà été configurés avec l'option par défaut (Réseau/Port). Ajoutez de nouveaux jeux de variables si vous souhaitez modifier la configuration par défaut.

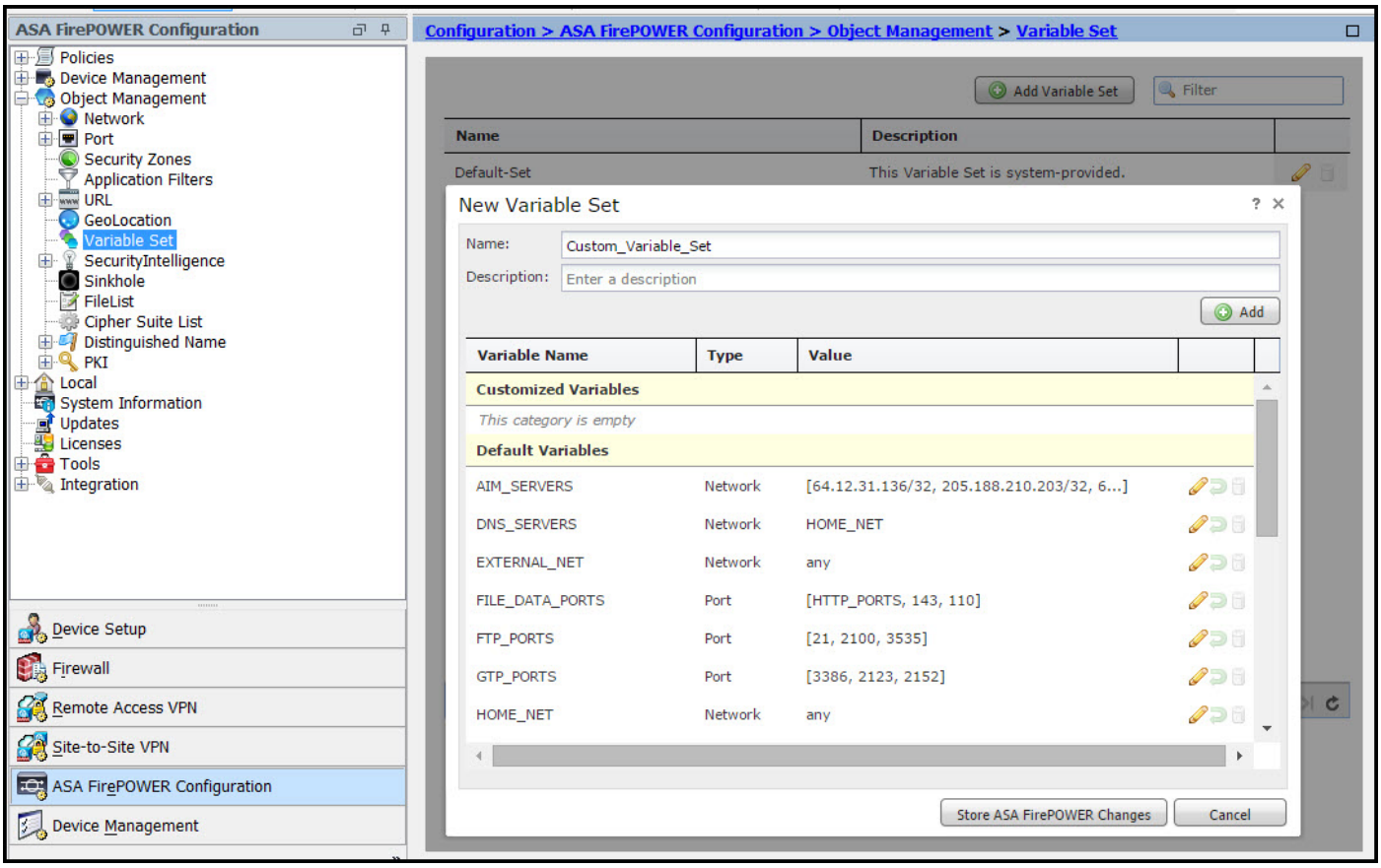
Pour configurer les jeux de variables, accédez à **Configuration > ASA Firepower Configuration > Object Management > Variable Set**. Sélectionnez l'option **Ajouter un jeu de variables** pour ajouter de nouveaux jeux de variables. Entrez le **nom** des jeux de variables et spécifiez la **description.**

Si une application personnalisée fonctionne sur un port spécifique, définissez le numéro de port

dans le champ Port number. Configurez le paramètre réseau.

$Home_NET spécifie le réseau interne.

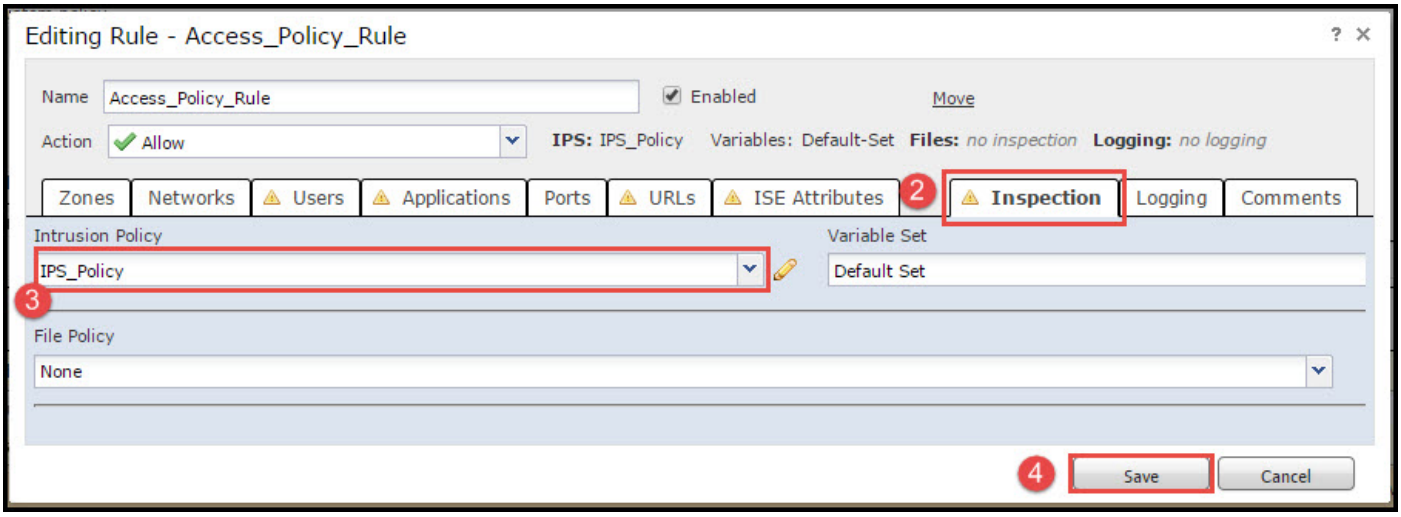
$External_NET spécifie le réseau externe.



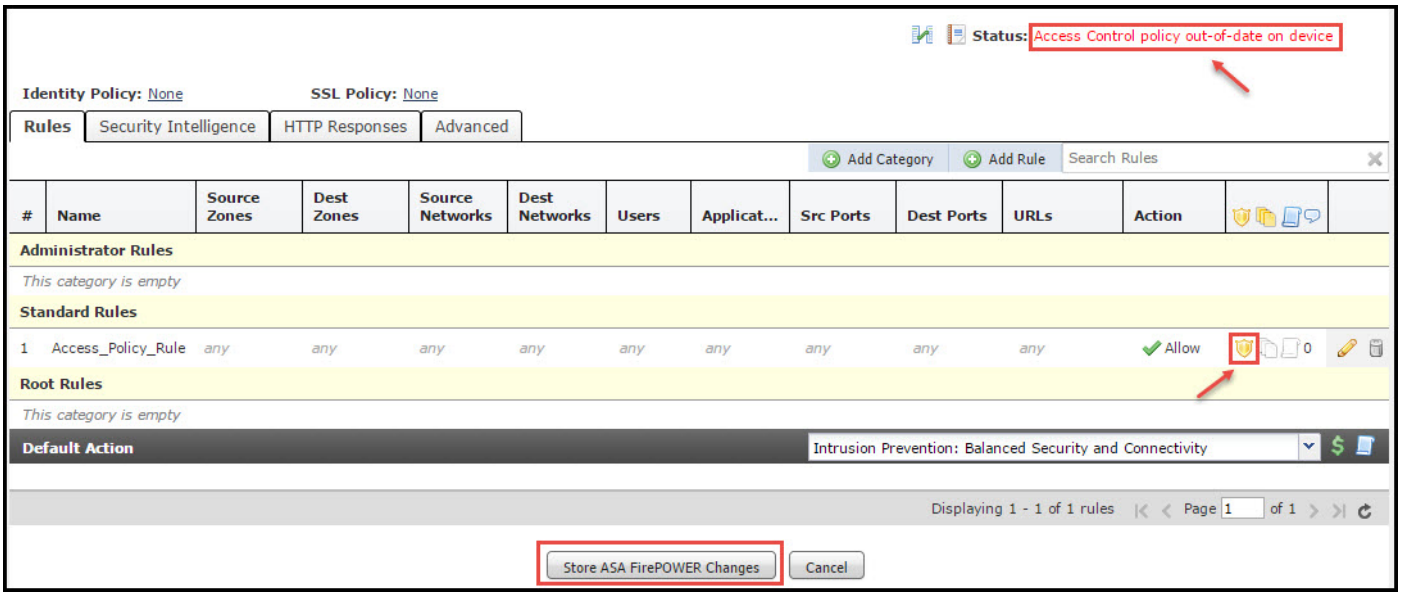
Étape 3 : Configurer le contrôle d'accès pour inclure la stratégie d'intrusion/les jeux de variables NAP/NAP

Accédez à **Configuration > ASA Firepower Configuration > Policies > Access Control Policy.** Vous devez effectuer les étapes suivantes :

1. Modifiez la règle de stratégie d'accès à l'endroit où vous voulez affecter la stratégie d'intrusion.
2. Sélectionnez l'onglet **Inspection.**
3. Choisissez la **stratégie d'intrusion** dans la liste déroulante et choisissez les **jeux de variables** dans la liste déroulante.
4. Click Save.



Depuis qu'une stratégie d'intrusion est ajoutée à cette règle de stratégie d'accès. Vous pouvez voir l'icône de protection dans Couleur dorée qui indique que la stratégie d'intrusion est activée.

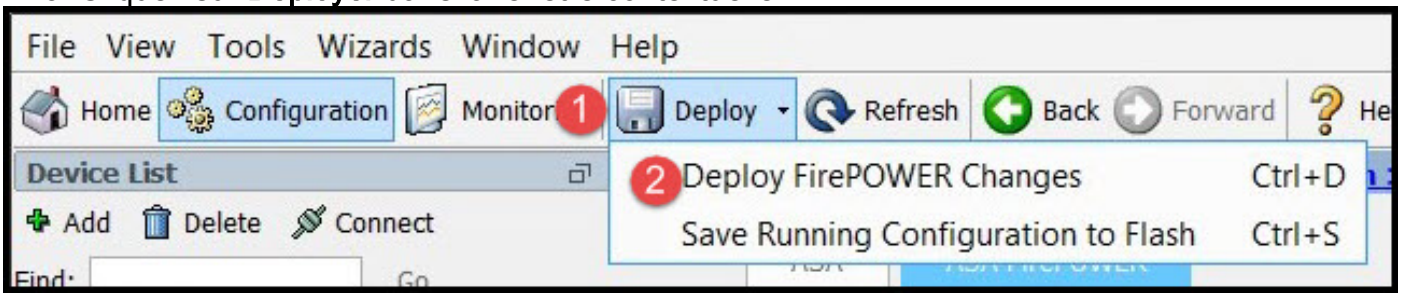


Cliquez sur **Store ASA FirePOWER changes** pour enregistrer les modifications.

Étape 4. Déployer la stratégie de contrôle d'accès

Désormais, vous devez déployer la stratégie de contrôle d'accès. Avant d'appliquer la stratégie, une indication de stratégie de contrôle d'accès est obsolète sur le périphérique. Pour déployer les modifications sur le capteur :

1. Cliquez sur **Déployer**.
2. Cliquez sur **Déployer les modifications FirePOWER**.
3. Cliquez sur **Déployer** dans la fenêtre contextuelle.

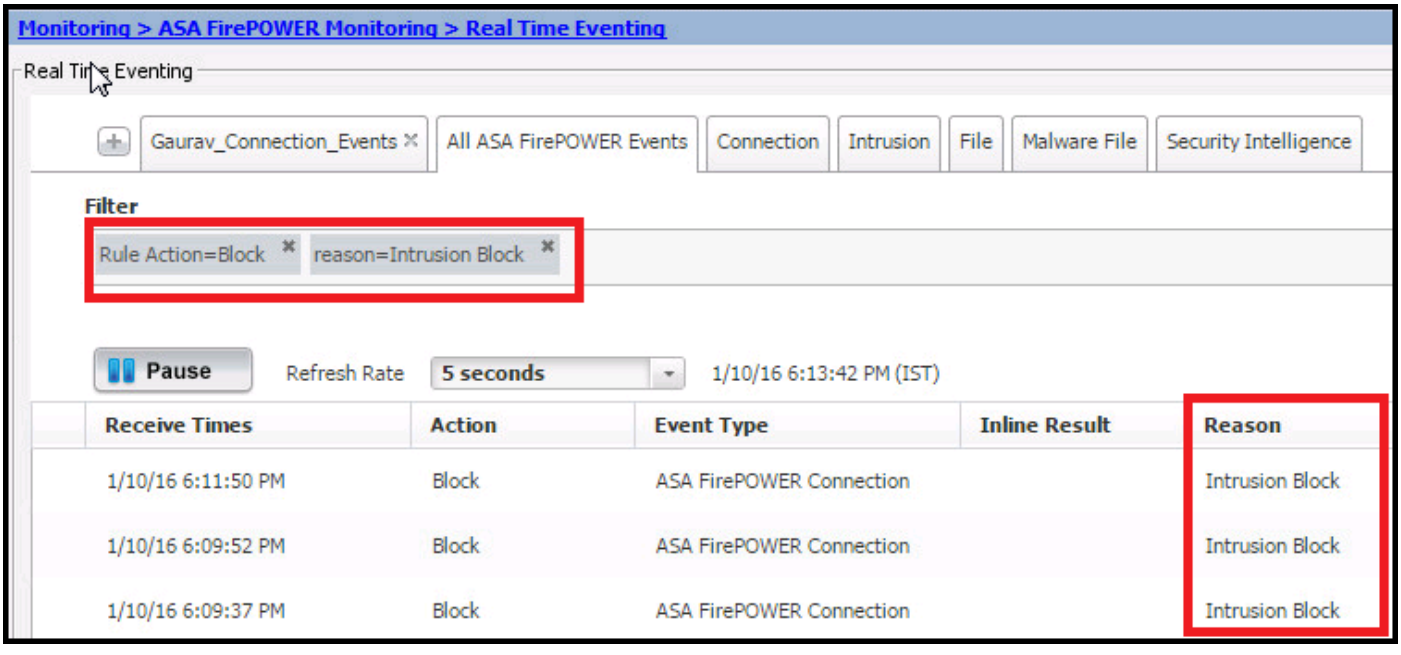


Remarque:: Dans la version 5.4.x, pour appliquer la stratégie d'accès au capteur, cliquez sur Apply ASA FirePOWER Changes.

Note: Accédez à **Monitoring > ASA Firepower Monitoring > Task Status.** Assurez-vous que la tâche doit être terminée pour appliquer la modification de configuration.

Étape 5. Surveiller les événements d'intrusion

Pour afficher les événements d'intrusion générés par le module FirePOWER, accédez à **Surveillance > ASA FirePOWER Monitoring > Real Time Evant.**



Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Étape 1. Assurez-vous que l'état des règles est correctement configuré.

Étape 2. Assurez-vous que la stratégie IPS correcte a été incluse dans les règles d'accès.

Étape 3. Assurez-vous que les jeux de variables sont configurés correctement. Si les jeux de variables ne sont pas configurés correctement, les signatures ne correspondent pas au trafic.

Étape 4. Assurez-vous que le déploiement de la stratégie de contrôle d'accès s'est terminé correctement.

Étape 5. Surveillez les événements de connexion et d'intrusion pour vérifier si le flux de trafic atteint ou non la règle correcte.

Informations connexes

- **Guide de démarrage rapide du module Cisco ASA FirePOWER**
- **Support et documentation techniques - Cisco Systems**