Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Informations générales](#)
[Configuration](#)
[Étape 1. Configurez la stratégie d'intrusion](#)
[Étape 1.1. Créez la stratégie d'intrusion](#)
[Étape 1.2. Modifiez la stratégie d'intrusion](#)
[Étape 1.3. Modifiez la stratégie de base](#)
[Étape 1.4. Signature filtrant avec l'option de barre de filtre](#)
[Étape 1.5. Configurez l'état de règle](#)
[Étape 1.6. Le filtre d'événement configurent](#)
[Étape 1.7. Configurez l'état dynamique](#)
[Étape 2. Configurez la stratégie d'analyse réseau (PETIT SOMME) et la variable place (facultatif)](#)
[Étape 3 : Configurez le contrôle d'accès pour inclure les positionnements variables de PETIT SOMME de politique d'intrusion](#)
[Étape 4. Déployez la stratégie de contrôle d'accès](#)
[Étape 5. Surveillez les événements d'intrusion](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

Introduction

Ce document décrit la fonctionnalité de système de détection du Système de prévention d'intrusion (IPS) /Intrusion (ID) du module de puissance de feu et éléments de la diverse stratégie d'intrusion qui définissent une stratégie de détection dans le module de puissance de feu.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

* La connaissance du Pare-feu de l'appliance de sécurité adaptable (ASA), Adaptive Security Device Manager (ASDM).

* La connaissance d'appareils de puissance de feu.

Composants utilisés

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

logiciel suivantes :

Version de logiciel courante 5.4.1 des modules de puissance de feu ASA (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) et plus élevé.

Version de logiciel courante 6.0.0 du module de puissance de feu ASA (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) et plus élevé.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

La puissance de feu IDS/IPS est conçue pour examiner le trafic réseau et pour identifier tous les modèles malveillants (ou signatures) qui indiquent une attaque de réseau/système. Le module de puissance de feu fonctionne en mode d'ID si la service-stratégie de l'ASA spécifiquement est configurée autrement dans le mode moniteur (promiscueux), il fonctionne en mode intégré.

La puissance de feu IPS/IDS est une approche basée sur signature de détection. FirePOWERmodule en mode d'ID génère une alerte quand la signature apparie le trafic malveillant, tandis que le module de puissance de feu en mode IPS génère le trafic malveillant d'alerte et de bloc.

> Remarque: Assurez-vous que le module de puissance de feu doit avoir **pour protéger le** permis de configurer cette fonctionnalité. Pour vérifier le permis, naviguez vers **permis de configuration > de puissance de feu ASA configuration >.**

Configuration

Étape 1. Configurez la stratégie d'intrusion

Étape 1.1. Créez la stratégie d'intrusion

Pour configurer la stratégie d'intrusion, ouvrez une session à Adaptive Security Device Manager (

Étape 1. Naviguez vers la **configuration de configuration > de puissance de feu ASA > les stratégies > la stratégie d'intrusion > la stratégie d'intrusion**.

Étape 2. Cliquez sur la **stratégie de création**.

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

Étape 4. Écrivez la **description de la** stratégie d'intrusion (facultative).

Étape 5. Spécifiez la **baisse quand** option **intégrée**.

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

Étape 7. Le clic **créent la stratégie** pour se terminer la création de stratégie d'intrusion.

> **Conseil** : Relâchez quand l'option intégrée est cruciale dans certains scénarios quand le capteur est configuré en mode intégré et on l'exige pour ne pas relâcher le trafic quoiqu'il apparie une signature qui a une action de baisse.

Vous pouvez noter que la stratégie est configurée, cependant, elle n'est appliquée à aucun périphérique.

Étape 1.2. Modifiez la stratégie d'intrusion

Pour modifier la stratégie d'intrusion, naviguer vers la **configuration de configuration > de puissance de feu ASA > les stratégies > la stratégie d'intrusion > la stratégie d'intrusion** et choisi **éditez l'**option.

Étape 1.3. Modifiez la stratégie de base

La page de Gestion des stratégies d'intrusion

La stratégie de base en contient système-a fourni les stratégies, qui sont des stratégies intégrées.

1. Sécurité et Connectivité équilibrées : C'est une stratégie optimale en termes de Sécurité et Connectivité. Cette stratégie a environ 7500 règles activées, certains d'entre elles génèrent seulement des événements tandis que d'autres génèrent des événements aussi bien que tombent le trafic.
2. Sécurité au-dessus de Connectivité : Si votre préférence est Sécurité puis vous pouvez choisir la Sécurité au-dessus de la stratégie de Connectivité, qui augmente le nombre de règles activées.
3. Connectivité au-dessus de Sécurité : Si votre est Connectivité plutôt que Sécurité alors vous pouvez choisir la Connectivité au-dessus de la stratégie de sécurité qui réduira le nombre de règles activées.
4. Détection maximum - Sélectionnez cette stratégie pour obtenir la détection maximum.
5. Aucun Active de règle - Cette option désactive toutes les règles. Vous devez activer les règles manuellement basées sur votre stratégie de sécurité.

Étape 1.4. Signature filtrant avec l'option de barre de filtre

Naviguez vers l'option de **règles** dans le panneau de navigation et la page de Gestion de règle paraît. Il y a des milliers de la règle dans la base de données de règle. La barre de filtre fournit une bonne option de moteur de recherche de rechercher la règle efficacement.

Vous pouvez insérer n'importe quel mot clé dans la barre de filtre et le système saisit les résultats pour vous. S'il y a une condition requise de trouver la signature pour la vulnérabilité heartbleed de Secure Sockets Layer (SSL), vous pouvez mot clé de recherche heartbleed dans la barre de filtre et elle cherchera la signature pour la vulnérabilité heartbleed.

> **Conseil** : Si de plusieurs mots clé sont utilisés dans la barre de filtre puis le système les combine utilisant ET la logique pour créer un composé les recherchent.

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

Des règles sont efficacement divisées en plusieurs manières telles que basé sur des vulnérabilités de Microsoft de classifications de catégorie/la particularité de plate-forme vers de terre de Microsoft. Une telle association des règles aide le client à obtenir la signature droite d'une méthode facile et à aider le client à accorder efficacement les signatures.

Vous pouvez également rechercher avec le nombre CVE à trouver les règles qui les couvrent. Vous pouvez utiliser le **CVE de** syntaxe **: <cve-number>.**

Étape 1.5. Configurez l'état de règle

Naviguez vers l'option de **règles** dans le panneau de navigation et la page de Gestion de règle paraît. Sélectionnez les règles et choisissez l'**état de règle d'**option pour configurer l'état des règles. Il y a trois états qui peuvent être configurés pour une règle :

1. **Générez les événements :** Cette option génère des événements quand la règle apparie le trafic.

2. **Relâchez et générez les événements :** Cette option génère les événements et le trafic de tomber quand la règle apparie le trafic.

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

Étape 1.6.

L'importance d'un événement d'intrusion peut être basée sur la fréquence de l'occurrence, ou sur la source ou l'adresse IP de destination. Dans certains cas, vous ne pouvez pas s'inquiéter d'un événement jusqu'à ce qu'il se soit produit un certain nombre de fois. Par exemple, vous ne pourriez pas être concerné si quelqu'un des tentatives d'ouvrir une session à un serveur jusqu'à ce qu'ils échouent un certain nombre de fois. Dans d'autres cas, vous pourriez seulement devoir voir quelques occurrences de hit de règle pour vérifier s'il y a un problème répandu.

Il y a deux manières par lesquelles vous pouvez réaliser ceci :

1. Seuil d'événement.

2. Suppression d'événement.

Seuil d'événement

Vous pouvez placer les seuils qui dictent combien de fois un événement est affiché, basé sur le nombre d'occurrences. Vous pouvez configurer le seuillage par événement et par stratégie.

Étapes pour configurer le seuil d'événement :

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

Étape 2. Cliquez sur le **filtrage d'événement**.

Étape 3. Cliquez sur le **seuil**.

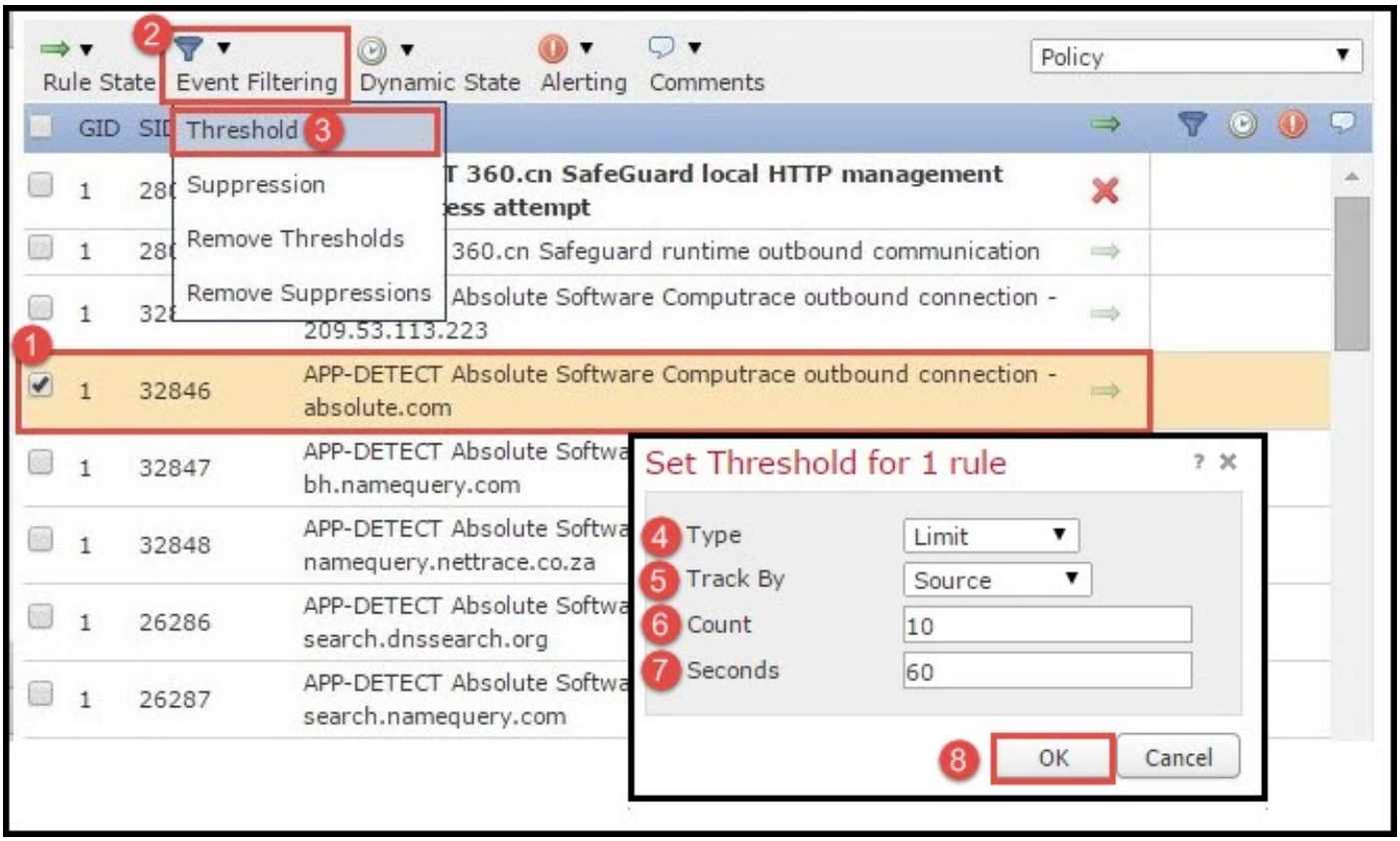
Étape 4. Sélectionnez le **type de la** liste déroulante. (Limite ou seuil ou chacun des deux).

Étape 5. Sélectionnez comment vous voulez dépister de la **piste par la** case de baisse. (Source ou destination).

Étape 6. Écrivez le **compte d'**événements pour rencontrer le seuil.

Étape 7. Écrivez les **secondes** pour s'écouler avant les remises de compte.

Étape 8. Cliquez sur OK pour se terminer.



Après qu'un filtre d'événement soit ajouté à une règle, vous devriez pouvoir voir une icône de filtre à côté de l'indication de règle, qui prouve qu'il y a un filtrage d'événement activé pour cette règle.

Suppression d'événement

Des notifications spécifiées d'événements peuvent être supprimées sur la base de l'adresse IP de destination de source ou par règle.

Remarque: Quand vous ajoutez la suppression d'événement pour une règle. L'inspection de signature fonctionne en tant que normalement mais le système ne génère pas les événements si le trafic apparie la signature. Si vous spécifiez une source/destination spécifiques puis les événements n'apparaissent pas seulement pour la source/destination spécifiques pour cette règle. Si vous choisissez de supprimer la règle complète puis le système ne génère aucun événement pour cette règle.

Étapes pour configurer le seuil d'événement :

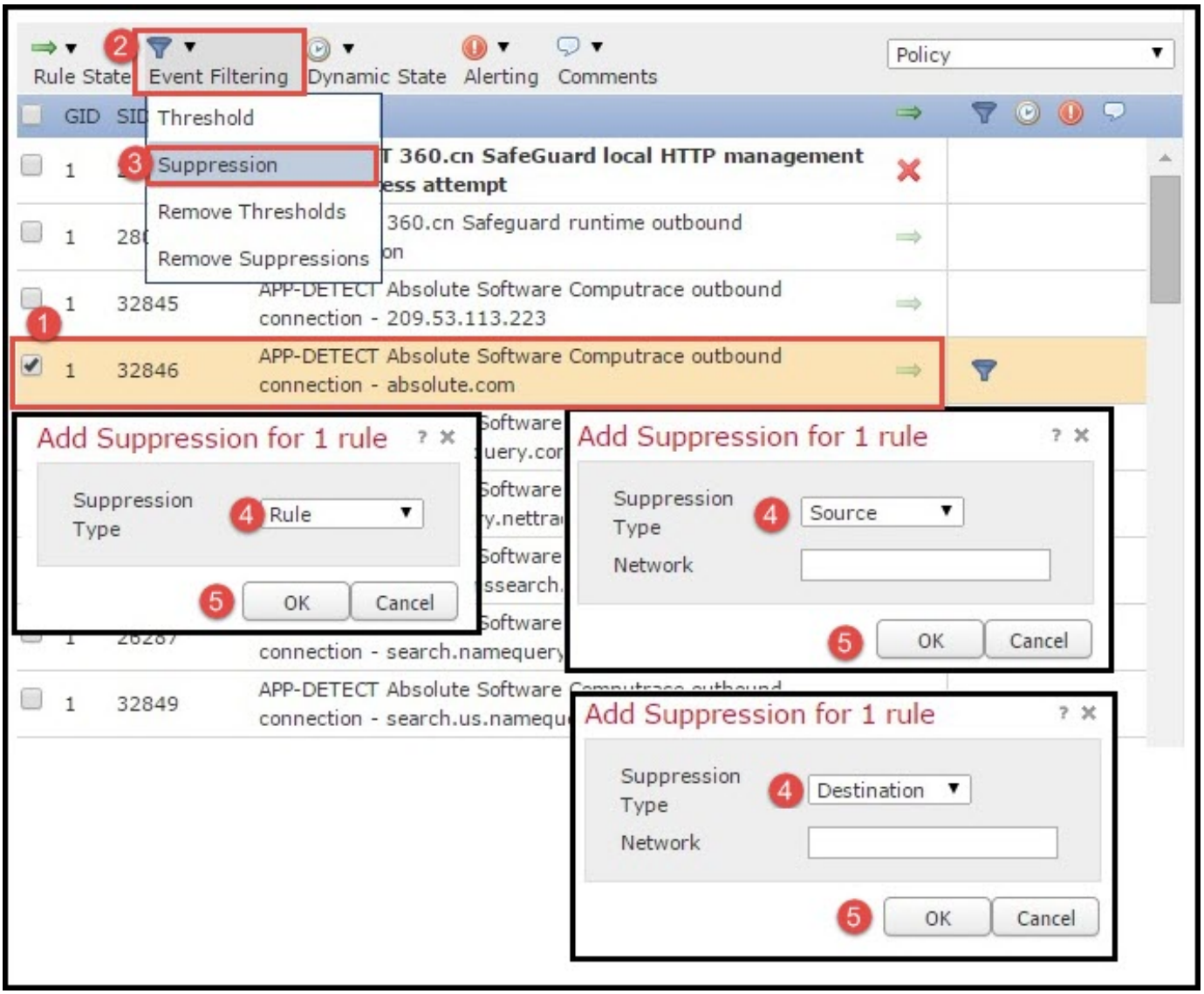
Étape 1. Sélectionnez les **règles** pour lesquelles vous voulez configurer le seuil d'événement.

Étape 2. **Filtrage d'événement de** clic.

Étape 3. **Suppression de** clic**.**

Type de suppression de l'étape 4.Select de la liste déroulante**.** (Règle ou source ou destination).

Étape 5. Cliquez sur OK pour se terminer.



Après que le filtre d'événement soit ajouté à cette règle, vous devriez pouvoir voir une icône de filtre avec le compte deux à côté de l'indication de règle, qui prouve qu'il y a deux filtres d'événement activés pour cette règle.

Étape 1.7. Configurez l'état dynamique

C'est une caractéristique où nous pouvons changer l'état d'une règle si l'état spécifié s'assortit.

Supposez un scénario d'attaque de force brutale pour fendre le mot de passe. Si une signature la détecte la tentative d'échouer de mot de passe et l'action de règle est de générer un événement. Le système continue à générer l'alerte pour la tentative d'échouer de mot de passe. Pour cette situation, vous pouvez utiliser l'**état dynamique** où une action des **événements Generate** peut être changée **pour relâcher et générer des événements** pour bloquer l'attaque de force brutale.

Naviguez vers l'option de **règles** dans le panneau de navigation et la page de Gestion de règle paraît. Sélectionnez la règle pour laquelle vous voulez activer l'état dynamique et choisir l'**état dynamique d'**options **> ajoutez un état de règle de Débit-base.**

Pour configurer l'état basé sur débit de règle :

1. Sélectionnez les **règles** pour lesquelles vous voulez configurer le seuil d'événement.
2. Cliquez sur l'**état dynamique**.
3. Cliquez sur l'**état basé sur débit de règle d'ajouter**.
4. Sélectionnez comment vous voulez dépister l'état de règle de la **piste par la** case de baisse. (**Règle ou source ou destination**).
5. Entrez dans le **réseau**. Vous pouvez spécifier une adresse IP simple, le bloc d'adresses, la variable, ou une virgule ? liste séparée qui est composée de n'importe quelle combinaison de ces derniers.
6. Écrivez le **compte d'**événements et l'horodateur en quelques secondes.
7. Sélectionnez le **nouvel état,** vous veulent définir pour la règle.
8. Écrivez le **délai d'attente** après quoi l'état de règle est retourné.
9. Cliquez sur **OK** pour terminer.

Étape 2. Configurez la stratégie d'analyse réseau (PETIT SOMME) et la variable place (facultatif)

Stratégie d'analyse de configure network

La stratégie d'accès au réseau est également connue comme préprocesseurs. Le préprocesseur fait le remontage de paquet et normalise le trafic. Il aide à identifier des anomalies de couche réseau et de protocole de la couche transport sur l'identification des options inadéquates d'en-tête.

Le PETIT SOMME fait le defragmentation des datagrammes IP, fournit l'inspection avec état de TCP et le réassemblage de flot et des sommes de contrôle de validation. Le préprocesseur normalise le trafic, valide et vérifie la norme de protocole.

Chaque préprocesseur a son propre nombre GID. Il représente quel préprocesseur a été déclenché par le paquet.

Àla stratégie d'analyse de configure network, naviguez vers la **configuration de configuration > de**

puissance de feu ASA > les stratégies > la stratégie de contrôle d'accès > a avancé > analyse réseau et stratégie d'intrusion

La stratégie par défaut d'analyse réseau est Sécurité et Connectivité équilibrées qui est stratégie recommandée optimale. Il y a trois autres stratégies supplémentaires de PETIT SOMME fournies par système qui peuvent être sélectionnées de la liste déroulante.

Liste choisie de **stratégie d'analyse réseau d'**option pour créer la stratégie faite sur commande de PETIT SOMME.

Configurez les positionnements variables

Des positionnements variables sont utilisés dans des règles d'intrusion d'identifier la source et les adresses de destination et les ports. Les règles sont plus efficaces quand les variables reflètent votre environnement de réseau plus exactement. La variable joue un important rôle dans l'optimisation des performances.

Des positionnements variables ont été déjà configurés avec l'option par défaut (réseau/port). Ajoutez les nouveaux positionnements variables si vous voulez changer la configuration par défaut.

Pour configurer les positionnements de variable, naviguez vers la **configuration de configuration > de puissance de feu ASA > la Gestion d'objet > le positionnement de variable**. L'option choisie **ajoutent le positionnement de variable** pour ajouter de nouveaux positionnements variables. Écrivez le **nom des** positionnements variables et spécifiez la **description.**

Si n'importe quelle application personnalisée travaille à un port spécifique alors définit le numéro de port dans le domaine de numéro de port. Configurez le paramètre de réseau.

$Home_NET spécifient le réseau interne.

$External_NET spécifient le réseau externe.

Étape 3 : Configurez le contrôle d'accès pour inclure les positionnements variables de PETIT SOMME de politique d'intrusion

Naviguez vers la **configuration de configuration > de puissance de feu ASA > les stratégies > la stratégie de contrôle d'accès.** Vous devez se terminer ces étapes :

1. Éditez la règle de stratégie d'Access où vous voulez assigner la stratégie d'intrusion.
2. Choisissez l'onglet d'**inspection**.
3. Choisissez la **stratégie d'intrusion de la** liste déroulante et choisissez les **positionnements variables de la** liste déroulante
4. Cliquez sur **Save**.

Puisqu'une stratégie d'intrusion est ajoutée à cette règle de stratégie d'Access. Vous pouvez voir l'icône de bouclier dans la couleur d'or qui indique que la stratégie d'intrusion est activée.

La puissance de feu de la mémoire ASA de clic **change** pour sauvegarder les modifications.

Étape 4. Déployez la stratégie de contrôle d'accès

Maintenant, vous devez déployer la stratégie de contrôle d'accès. Avant que vous appliquiez la stratégie, vous verrez une stratégie de contrôle d'accès d'indication périmée sur le périphérique. Pour déployer les modifications au capteur :

1. Le clic **se déploient**.
2. Le clic **déploient des modifications de puissance de feu**.
3. Le clic **se déploient** dans la fenêtre externe.

Remarque: Dans la version 5.4.x, pour appliquer la stratégie d'accès au capteur, vous devez cliquer sur Apply des modifications de puissance de feu ASA

Remarque: Naviguez vers la **surveillance > surveillance de puissance de feu ASA > état de tâche.** Assurez-vous que la tâche doit se terminer pour appliquer la modification de configuration.

Étape 5. Surveillez les événements d'intrusion

Pour voir les événements d'intrusion générés par le module de puissance de feu, naviguez vers la **surveillance > surveillance de puissance de feu ASA > concours complet en temps réel.**

Vérifiez

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

Dépannez

Étape 1. Assurez-vous que l'état de règle de règles est convenablement configuré.

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

Étape 3. Assurez-vous que des positionnements de variables sont configurés correctement. Si les positionnements variables ne sont pas configurés correctement puis les signatures n'apparieront pas le trafic.

Étape 4. Assurez-vous que le déploiement de stratégie de contrôle d'accès se termine avec succès.

Étape 5. Surveillez les événements de connexion et les événements d'intrusion pour vérifier si la circulation frappe la règle correcte ou pas.

Informations connexes

- **Guide de démarrage rapide de module de puissance de feu de Cisco ASA**
- **Support et documentation techniques - Cisco Systems**