Configurez l'IP mettant sur la liste noire tout en utilisant l'intelligence de sécurité Cisco par ASDM (la Gestion de Sur-case)

Contenu

Introduction

Ce document décrit la réputation d'intelligence/adresse IP de sécurité Cisco et la configuration de l'IP mettant sur la liste noire (blocage) tandis que flux fait sur commande/automatique d'utilisation de la basse adresse IP de réputation.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du Pare-feu ASA (appliance de sécurité adaptable), ASDM (Adaptive Security Device Manager)
- La connaissance d'appareils de puissance de feu

Remarque: Le filtrage de renseignements de sécurité exige un permis de protection.

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 en haut
- 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 en haut

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

L'intelligence de sécurité Cisco comporte de plusieurs collections d'adresses IP régulièrement à jour qui sont déterminées pour avoir une réputation pauvre par l'équipe de Cisco TALOS. L'équipe de Cisco TALOS détermine la basse réputation si n'importe quelle action malveillante est provenue de ces adresses IP telles que les Spam, le malware, les attaques par phishing etc.

Le flux d'intelligence de sécurité IP de Cisco dépiste la base de données des attaquants, Bogon, des robots, commande numérique par ordinateur, Dga, ExploitKit, malware, Open_proxy, Open_relay, phishing, réponse, Spam, méfiant. Le module de puissance de feu fournit l'option de créer le flux fait sur commande de la basse adresse IP de réputation.

Aperçu de flux de renseignements de sécurité

Voici encore plus d'informations sur le type de collections d'adresse IP qui peuvent être classifiées comme catégories différentes dans les renseignements de sécurité.

Attaquants : Collecte d'adresses IP qui continuellement balayent pour des vulnérabilités ou tentent d'exploiter d'autres systèmes.

Malware : Collecte d'adresses IP qui tentent de propager le malware ou attaquent activement n'importe qui qui les visite.

Phishing : Collecte d'hôtes qui tentent activement de duper des utilisateurs finaux dans écrire les informations confidentielles comme des noms d'utilisateur et mot de passe.

Spam : Collecte d'hôtes qui ont été identifiés comme la source d'envoyer des messages électroniques de Spam.

Robots : La collecte d'hôtes qui participent activement en tant qu'élément d'un botnet, et sont contrôlées par un contrôleur connu de net de robot.

Commande numérique par ordinateur : Collecte d'hôtes qui ont été identifiés en tant que serveurs de contrôle pour un Botnet connu.

OpenProxy : Collecte d'hôtes qui sont connus pour exécuter des proxys ouverts de Web et pour offrir des services anonymes de navigation web.

OpenRelay : La collecte d'hôtes qui sont connus pour offrir l'email anonyme transmettant par relais des services l'a utilisé par des attaquants de Spam et de phishing.

TorExitNode : Collecte d'hôtes qui sont connus pour offrir des services de noeud de sortie pour le réseau d'Anonymizer de massif de roche.

Bogon : La collecte d'adresses IP qui ne sont pas allouées mais envoient le trafic.

Méfiant : Collecte d'adresses IP qui affichent l'activité suspecte et sont sous l'enquête active.

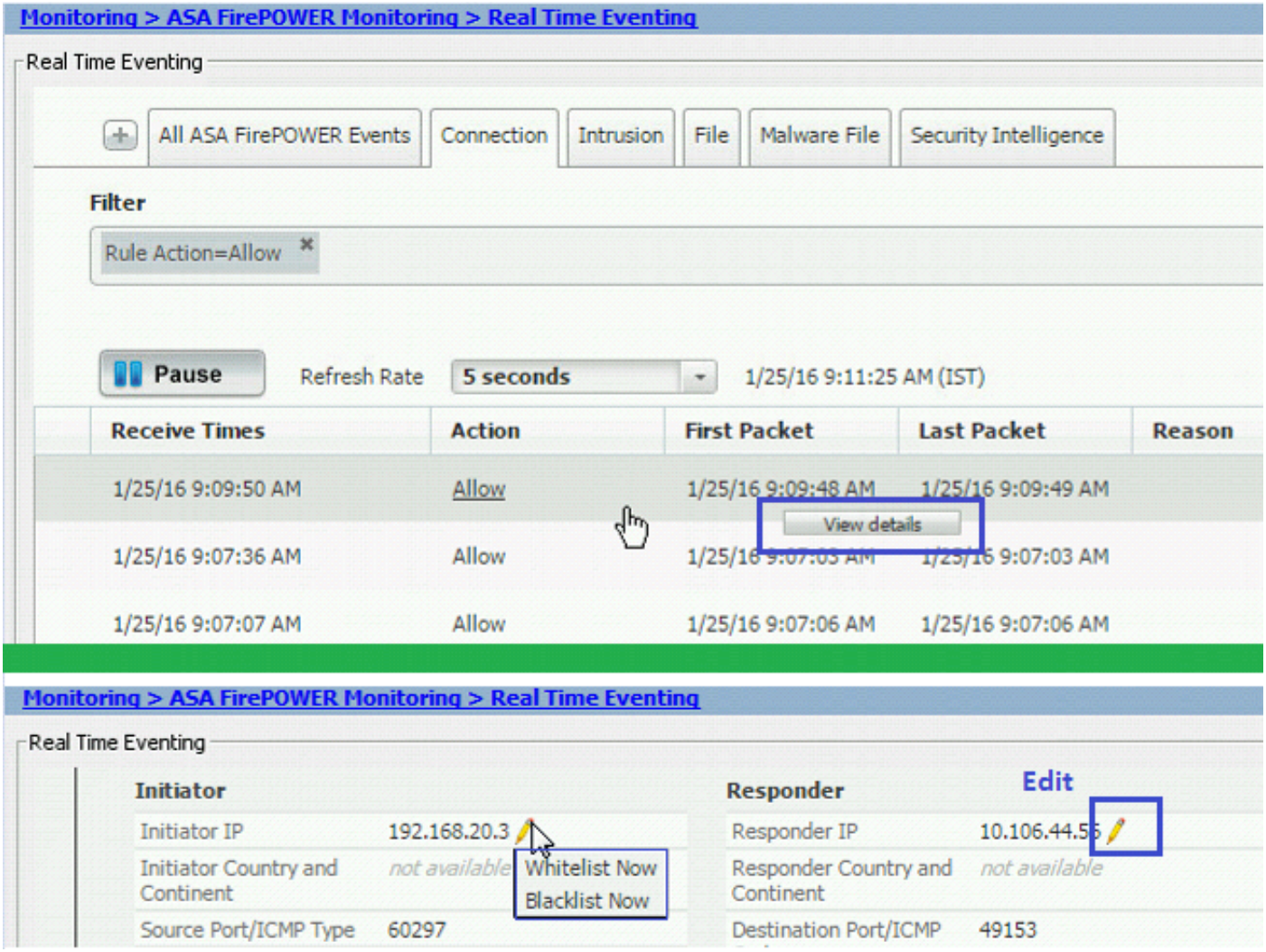
Réponse : Collecte d'adresses IP qui ont été à plusieurs reprises observées occupées dans le comportement méfiant ou malveillant.

Ajoutez manuellement la Global-liste noire d'adresses IP et global-Whitelist

Le module de puissance de feu te permet pour ajouter certaine Global-liste noire d'adresses IP quand vous savez qu'ils font partie d'une certaine action malveillante. Des adresses IP peuvent également être ajoutées à global-Whitelist, si vous voulez permettre le trafic à certaines adresses IP qui sont bloquées par des adresses IP de liste noire. Si vous ajoutez n'importe quelle Global-liste noire d'adresse IP/global-Whitelist, elle la prend effet immédiatement sans nécessité d'appliquer la stratégie.

Afin d'ajouter l'adresse IP à Global-Blacklist/global-Whitelist, naviguez vers la **surveillance > surveillance de puissance de feu ASA > concours complet en temps réel**, passer au-dessus la souris sur des événements de connexion et sélectionnez les **détails de vue**.

Vous pouvez ajouter la source ou l'adresse IP de destination au Global-Blacklist/global-Whitelist. Cliquez sur en fonction le bouton **Edit** et **maintenant** choisi de **Whitelist/liste noire maintenant** pour ajouter l'adresse IP à la liste respective, suivant les indications de l'image.



Afin de vérifier que la source ou l'adresse IP de destination est ajoutée au Global-Blacklist/global-Whitelist, naviguez vers la **configuration de configuration > de puissance de feu ASA > la Gestion > les renseignements de sécurité > les listes des réseaux et les flux d'objet** et éditez **Global-Blacklist/Whitelist global**. Vous pouvez également utiliser le bouton d'effacement pour retirer n'importe quelle adresse IP de la liste.

Créez la liste faite sur commande d'adresse IP de liste noire

La puissance de feu te permet pour créer la liste faite sur commande de réseau/adresses IP qui peut être utilisée en mettant sur la liste noire (blocage). Il y a l'option trois de faire ceci :

1. Vous pouvez écrire les adresses IP à un fichier texte (une adresse IP par la ligne) et pouvez télécharger le fichier au module de puissance de feu. Afin de télécharger le fichier, naviguez vers la **configuration de configuration > de puissance de feu ASA > la Gestion > les renseignements de sécurité > les listes des réseaux et les flux d'objet** et puis cliquez sur Add les **listes des réseaux et les flux** **Nom :** Spécifiez le nom de la liste faite sur commande. **Type :** Sélectionnez la **liste de la** liste déroulante. **Liste de téléchargement :** Choisissez **parcourent** pour localiser le fichier texte dans votre système. **Téléchargement** choisi d'option pour télécharger le fichier.
2. Vous pouvez utiliser n'importe quelle base de données IP de tierce partie pour la liste faite sur commande pour laquelle le module de puissance de feu contacte le serveur de tiers pour chercher la liste d'adresse IP. Afin de configurer ceci, naviguez vers la **configuration de**

configuration > de puissance de feu ASA > la Gestion > les renseignements de sécurité > les listes des réseaux et les flux d'objet et puis cliquez sur Add les **listes des réseaux et les flux**

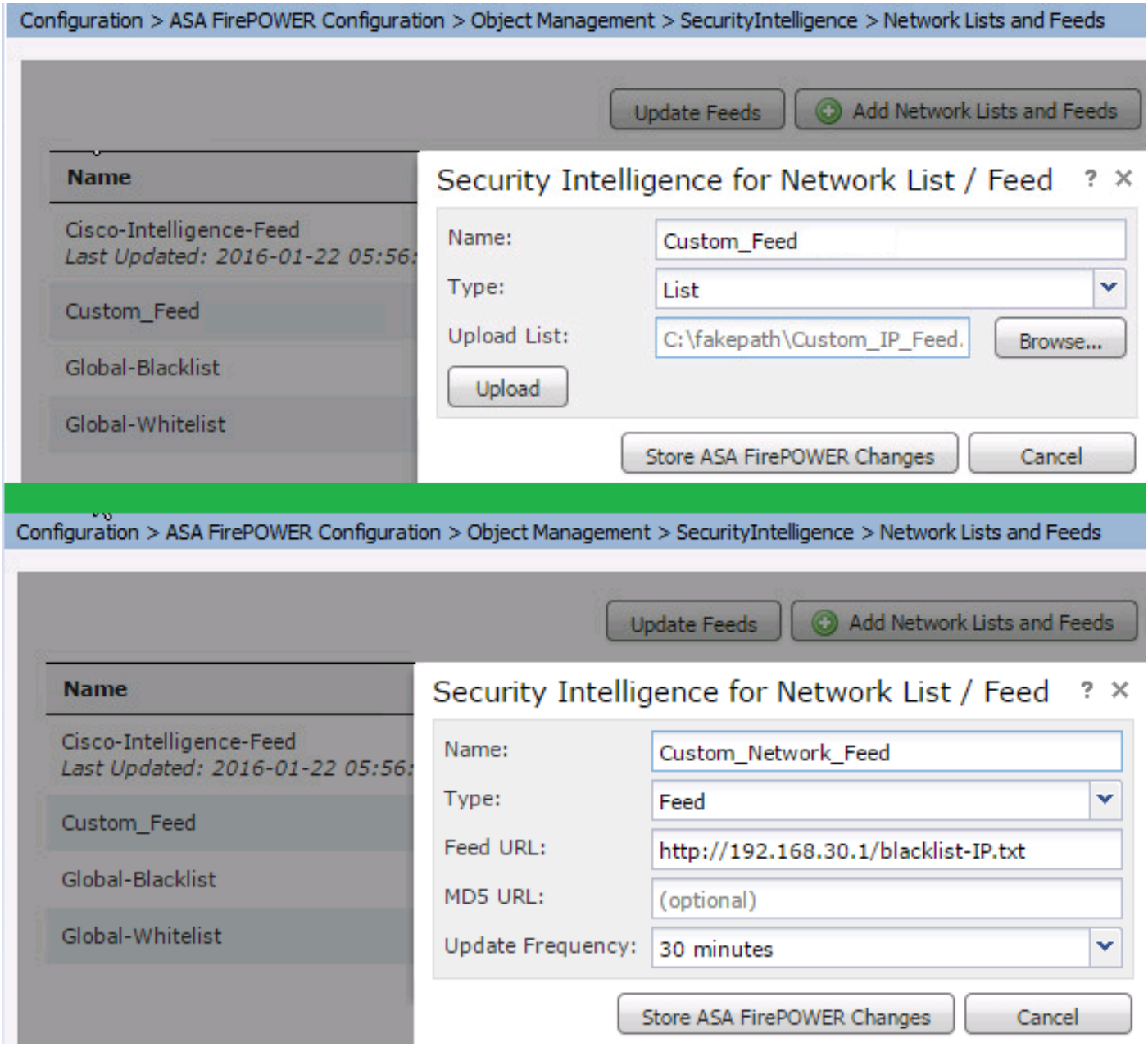
Nom : Spécifiez le nom du flux fait sur commande.

Type : Flux choisi d'option de la liste déroulante.

URL de flux : Spécifiez l'URL du serveur auquel le module de puissance de feu devrait se connecter et téléchargez le flux.

URL DE MD5 : Spécifiez la valeur de hachage pour valider le chemin URL de flux.

Fréquence de mise à jour : Spécifiez l'intervalle de temps en lequel le système se connectent au serveur de flux URL.



Configurez les renseignements de sécurité

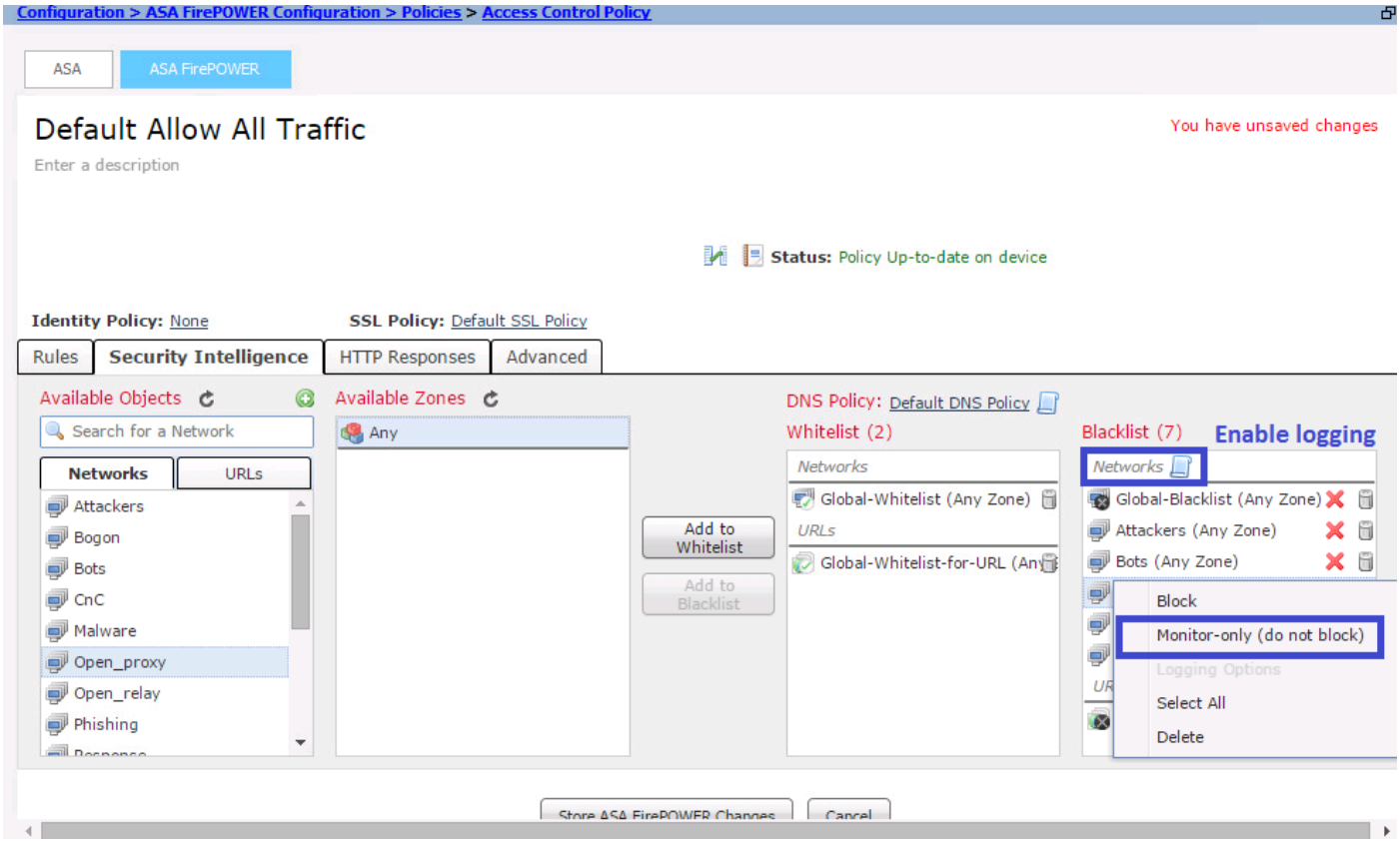
Afin de configurer des renseignements de sécurité, naviguez vers la **configuration de configuration > de puissance de feu ASA > les stratégies > la stratégie de contrôle d'accès,** onglet choisi de

renseignements de sécurité.

Choisissez le flux de l'objet disponible de réseau, mouvement au au laisser de colonne de **liste noire Whitelist**/pour/bloc la connexion à l'adresse IP malveillante.

Vous pouvez cliquer sur l'icône et activer se connecter comme spécifié dans l'image.

Si vous voulez juste générer l'événement pour les connexions malveillantes IP au lieu de bloquer la connexion, alors cliquez avec le bouton droit sur le flux, choisissent **réservé au moniteur (ne font pas le bloc)**, suivant les indications de l'image :

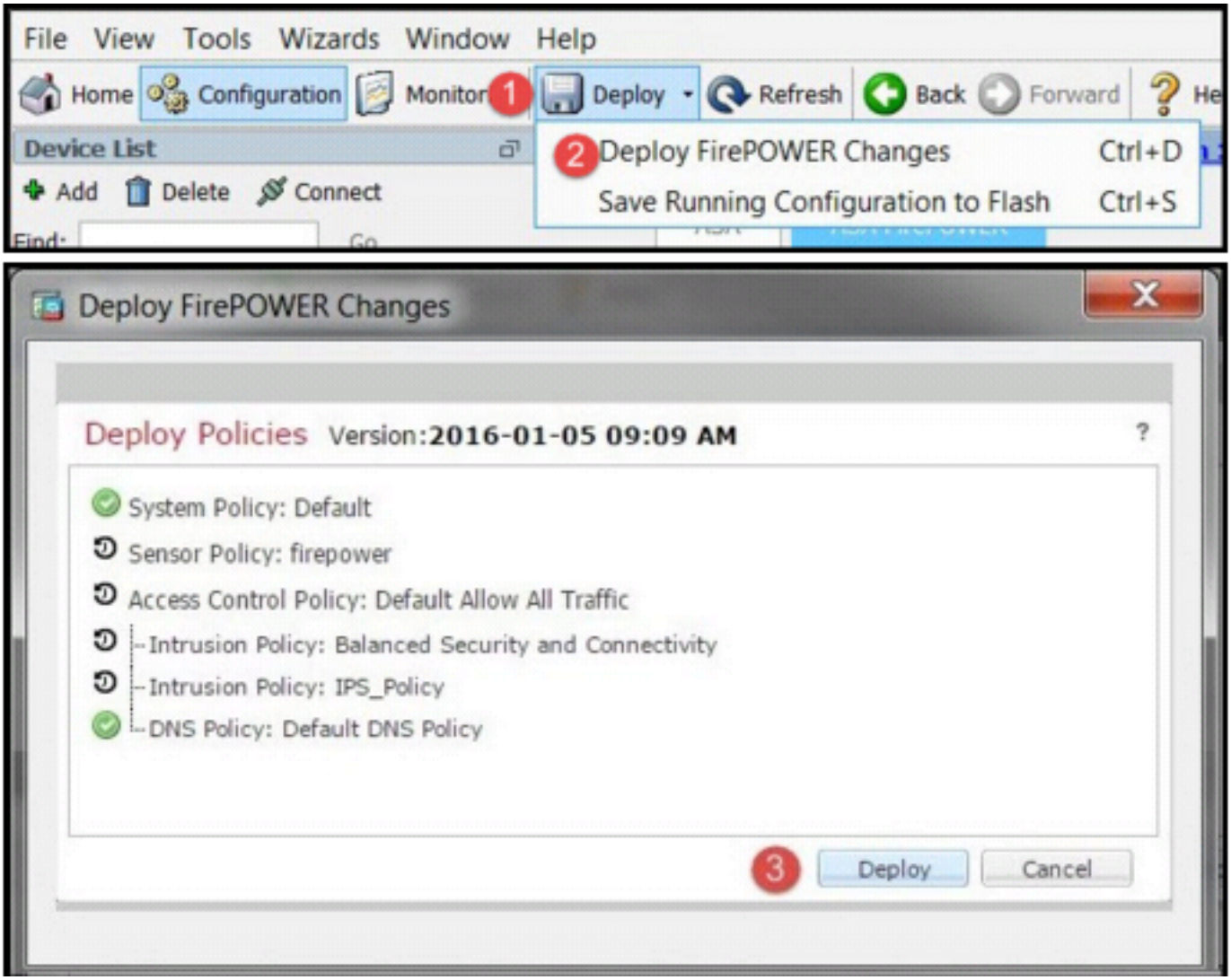


Choisissez les modifications de puissance de feu de la mémoire ASA d'option pour sauvegarder les changements de politique à C.A.

Déployez la stratégie de contrôle d'accès

Pour que les modifications les prennent effet, vous devez déployer la stratégie de contrôle d'accès. Avant que vous appliquiez la stratégie, voir l'indication qui, que la stratégie de contrôle d'accès soit périmée sur le périphérique ou pas.

Pour déployer les modifications au capteur, le clic **se déploient** et choisissent **déploient des modifications de puissance de feu** puis les sélectionnent **se déploient** dans la fenêtre externe pour déployer les modifications.

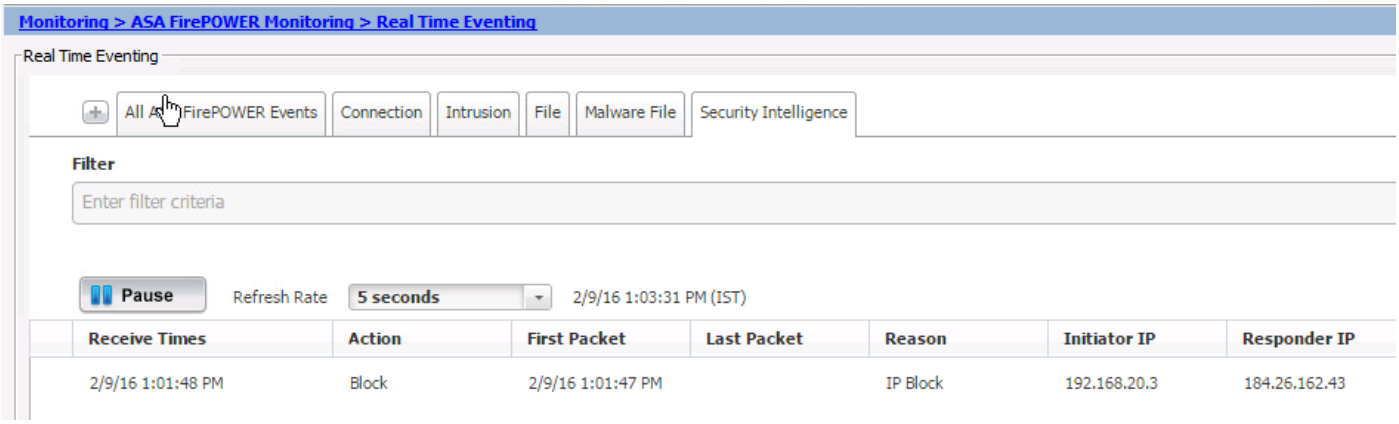


Remarque: Dans la version 5.4.x, pour appliquer la stratégie d'accès au capteur, vous devez cliquer sur Apply des **modifications de puissance de feu ASA**

Remarque: Naviguez vers la **surveillance > surveillance de puissance de feu ASA > état de tâche.** Assurez-vous que la tâche doit se terminer afin d'appliquer les modifications de configuration.

Surveillance des événements des renseignements de sécurité

Afin de voir les renseignements de sécurité par le module de puissance de feu, naviguez vers la **surveillance > surveillance de puissance de feu ASA > concours complet en temps réel**. Sélectionnez l'onglet de **renseignements de sécurité**. Ceci révélera les événements suivant les indications de l'image :

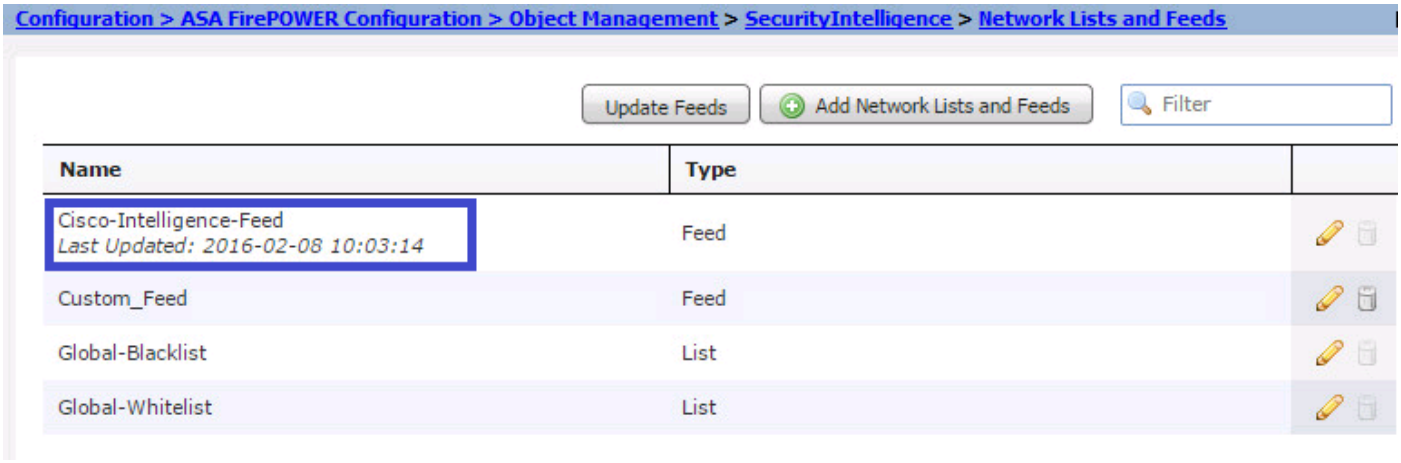


Vérifiez

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

Dépannez

Afin de s'assurer que les flux de renseignements de sécurité est à jour, naviguez vers la **configuration de configuration > de puissance de feu ASA > la Gestion > les renseignements de sécurité > les listes des réseaux et les flux d'objet** et vérifiez le moment où le flux a été pour la dernière fois mis à jour. Vous pouvez choisir le bouton d'éditer pour placer la fréquence de la mise à jour de flux.



Assurez-vous que le déploiement de stratégie de contrôle d'accès s'est terminé avec succès.

Surveillez les renseignements de sécurité de voir si le trafic bloque ou pas.

Informations connexes

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