Configurez le module de FirePOWER pour l'AMP de réseau ou le contrôle de fichier avec l'ASDM.

Contenu

Introduction

Ce document décrit la fonctionnalité de contrôle d'accès de protection de malware avancée par réseau (AMP) /file du module de FirePOWER et de la méthode pour les configurer avec Adaptive Security Device Manager (ASDM).

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) et de l'ASDM.
- La connaissance d'appareils de FirePOWER.

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 ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) et plus tard.
- Module ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) cette version de logiciel 6.0.0 de passage et plus tard.

- ASDM 7.5.1 et plus tard.

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

Le logiciel/malware malveillants peut entrer dans le réseau d'une organisation par l'intermédiaire de plusieurs manières. Afin d'identifier et atténuer les effets de ces logiciel et malware malveillants, les caractéristiques de l'AMP de FirePOWER peuvent être utilisées afin de détecter et bloquer sur option la transmission du logiciel et du malware malveillants dans le réseau.

Avec la fonctionnalité de contrôle de fichier, vous pouvez choisir de surveiller (détecter), de bloquer, ou permettre le transfert du téléchargement de fichier et du téléchargement. Par exemple, on peut mettre en application une stratégie de fichier qui bloque le téléchargement des fichiers exécutables par l'utilisateur.

Avec la fonctionnalité d'AMP de réseau, vous pouvez sélectionner les types de fichier que vous souhaitez surveiller au-dessus des protocoles utilisés généralement et envoyer le SHA 256 hache, les métadonnées à partir des fichiers, ou même les copies des fichiers elles-mêmes au nuage d'intelligence de sécurité Cisco pour l'analyse de malware. La disposition de retours de nuage pour le fichier hache comme propre ou malveillant basé sur l'analyse de fichier.

Le contrôle et l'AMP de fichier pour FirePOWER peuvent être configurés comme stratégie de fichier et être utilisés en tant qu'élément de votre configuration globale de contrôle d'accès. Les stratégies de fichier associées avec des règles de contrôle d'accès examinent le trafic réseau que remplit des conditions de règle.

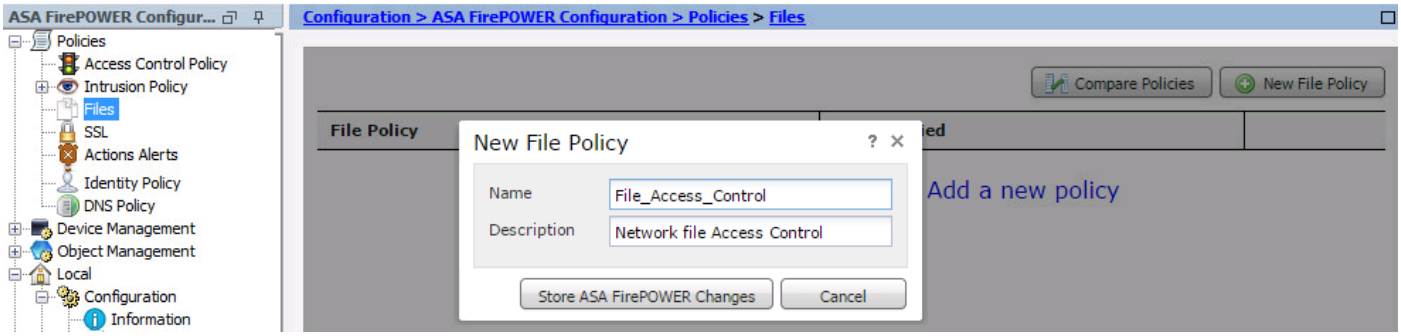
> **Note**: Assurez-vous que le module de FirePOWER a un permis de protection/contrôle/malware afin de configurer cette fonctionnalité. Afin de vérifier les permis, choisissez la **configuration > la configuration > le permis ASA FirePOWER.**

Configurez la stratégie de fichier pour l'AMP de contrôle/réseau de fichier

Configurez le contrôle d'accès de fichier

Ouvrez une session à l'ASDM et choisissez la **configuration > la configuration > les stratégies > les fichiers ASA FirePOWER.** La boîte de dialogue de **stratégie de nouveau fichier** apparaît.

Écrivez un nom et une description facultative pour votre nouvelle stratégie, puis cliquez sur l'option de **modifications de la mémoire ASA FirePOWER**. La page Règle de stratégie de fichier paraît.



Cliquez sur Add la **règle de fichier** afin d'ajouter une règle à la stratégie de fichier. La règle de fichier te donne le contrôle granulaire des types de fichier que vous voulez se connecter, bloquer, ou balayer pour le malware.

Protocole de l'application : Spécifiez le protocole de l'application en tant que (par défaut) ou le protocole spécifique (HTTP, SMTP, IMAP, POP3, FTP, PME).

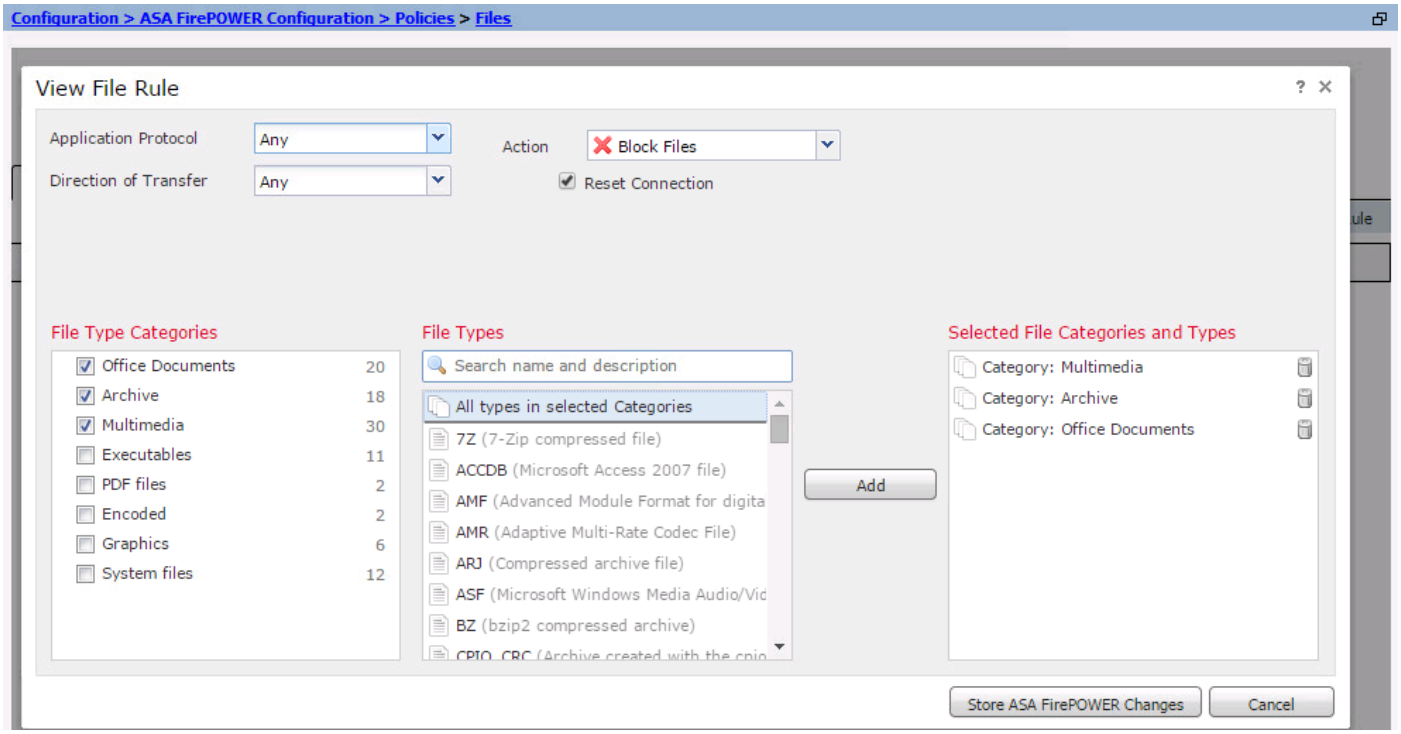
Direction de transfert : Spécifiez la direction du transfert de fichiers. C'en a pu être ou téléchargement/téléchargement basé sur le protocole de l'application. Vous pouvez examiner le protocole (HTTP, IMAP, POP3, FTP, PME) pour assurer le téléchargement de fichier et le protocole (HTTP, SMTP, FTP, PME) pour le téléchargement de fichier. Employez la **n'importe quelle** option afin de détecter des fichiers au-dessus des protocoles d'application multiple, indépendamment de si les utilisateurs envoient ou reçoivent le fichier.

Action : Spécifiez l'action pour la fonctionnalité de contrôle d'accès de fichier. L'action serait **détectent des fichiers** ou **bloquent des fichiers. Détectez l'**action de **fichier** génère l'événement et l'action de **fichiers de bloc** génèrent l'événement et bloquent la transmission de fichiers. Avec des **fichiers** action de **bloc**, vous pouvez sur option sélectionner la **connexion de remise** pour terminer la connexion.

Type de fichier catégories : Sélectionnez le type de fichier catégories pour lequel vous voulez au fichier de bloc ou générez l'alerte.

Types de fichier : Sélectionnez les types de fichier. Les types de fichier option donne une option plus granulaire de choisir le type de fichier spécifique.

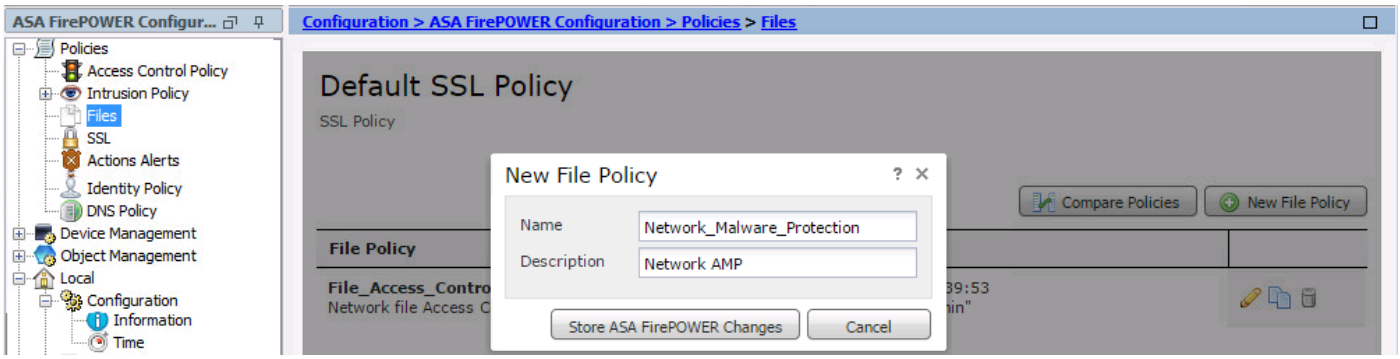
Choisissez l'option de **modifications de la mémoire ASA FirePOWER** de sauvegarder la configuration.



Protection de malware de configure network (AMP de réseau)

Ouvrez une session à l'ASDM et naviguez vers la **configuration > la configuration > les stratégies > les fichiers ASA FirePOWER.** La page de stratégie de fichier paraît. Cliquez sur maintenant en fonction la la boîte de dialogue de stratégie de nouveau fichier apparaît.

Écrivez un **nom** et une **description** facultative pour votre nouvelle stratégie, puis cliquez sur en fonction l'option de **modifications de la mémoire ASA FirePOWER**. La page de règles de stratégie de fichier paraît.



Cliquez sur l'option de **règle de fichier d'ajouter** d'ajouter une règle de classer la stratégie. La règle de fichier te donne le contrôle granulaire des types de fichier que vous voulez se connecter, bloquer, ou balayer pour le malware.

Protocole de l'application : En spécifiez (par défaut) ou le protocole spécifique (HTTP, SMTP, IMAP, POP3, FTP, la PME)

Direction de transfert : Spécifiez la direction du transfert de fichiers. C'en a pu être ou téléchargement de téléchargement basé sur le protocole de l'application. Vous pouvez examiner le protocole (HTTP, IMAP, POP3, FTP, PME) pour assurer le téléchargement de fichier et le protocole (HTTP, SMTP, FTP, PME) pour le téléchargement de fichier. Utilisez **n'importe quelle** option de détecter des fichiers au-dessus des protocoles d'application multiple, indépendamment des utilisateurs envoyant ou recevant le fichier.

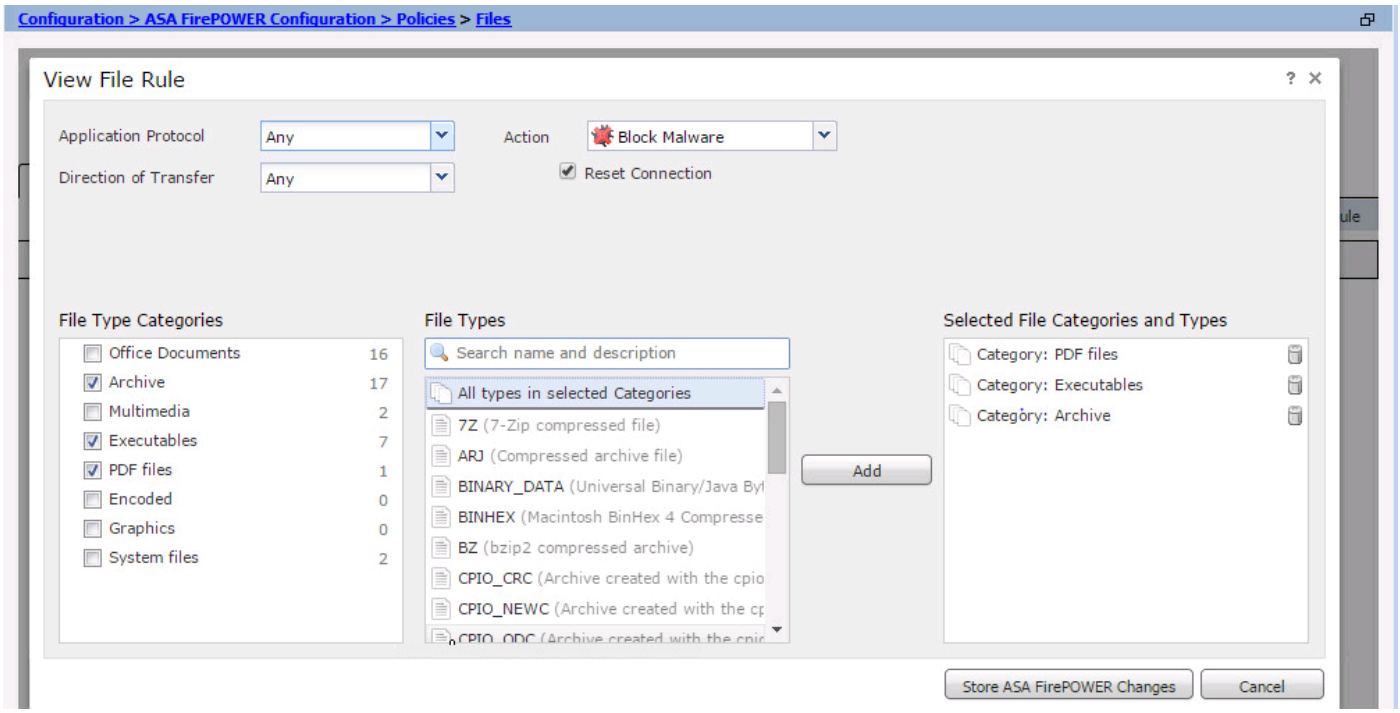
Action : Pour la fonctionnalité de protection de malware de réseau, l'action serait l'un ou l'autre de **consultation de nuage de malware** ou **bloquerait le malware. La consultation de nuage de malware d'**action génère seulement un événement tandis que le **malware de bloc d'**action génère l'événement aussi bien que bloque la transmission de fichiers de malware.

> **Note**: Les règles de **malware d'**andBlock de **consultation de nuage de malware** permettent à FirePOWER pour calculer les informations parasites SHA-256 et pour les envoyer pour que le processus de recherche de nuage détermine si les fichiers traversant le réseau contiennent le malware.

Type de fichier catégories : Sélectionnez les catégories de fichier spécifique.

Types de fichier : Sélectionnez les **types de** fichier spécifique pour des types de fichier plus granulaires.

Choisissez les **modifications de la mémoire ASA FirePOWER d'**option pour sauvegarder la configuration.

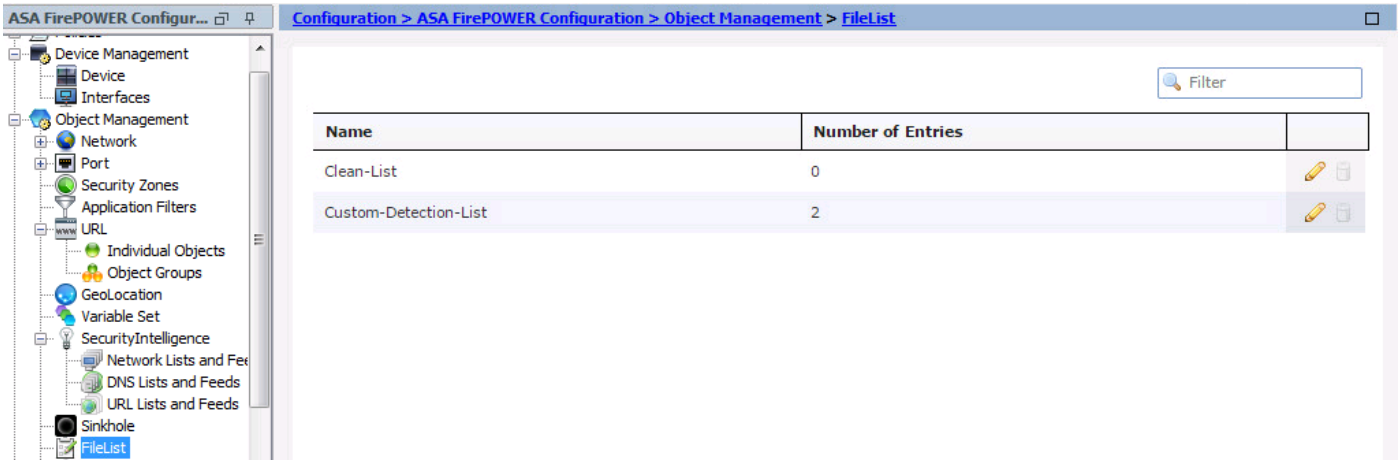


> **Note**: Les stratégies de fichier traitent des fichiers dans la commande suivante de règle-action : Le blocage a la priorité au-dessus de l'inspection de malware, qui a la priorité au-dessus de la détection et de se connecter simples.

Si vous configurez la protection avancée Fondé(e) sur le réseau de malware (AMP), et Cisco opacifient détecte inexactement la disposition d'un fichier, vous pouvez ajouter le fichier pour classer la liste utilisant une valeur de hachage SHA-256 pour s'améliorer détectez la disposition de fichier à l'avenir. selon le type de liste de fichier, vous pouvez faire :

- Pour traiter un fichier comme si le nuage a assigné une disposition propre, ajoutez le fichier à la liste propre.
- Pour traiter un fichier comme si le nuage a assigné une disposition de malware, ajoutez le fichier à la liste faite sur commande.

Pour configurer ceci, naviguer vers la **configuration > la configuration ASA FirePOWER > la Gestion d'objet > la liste de fichier** et éditer la liste pour ajouter SHA-256.



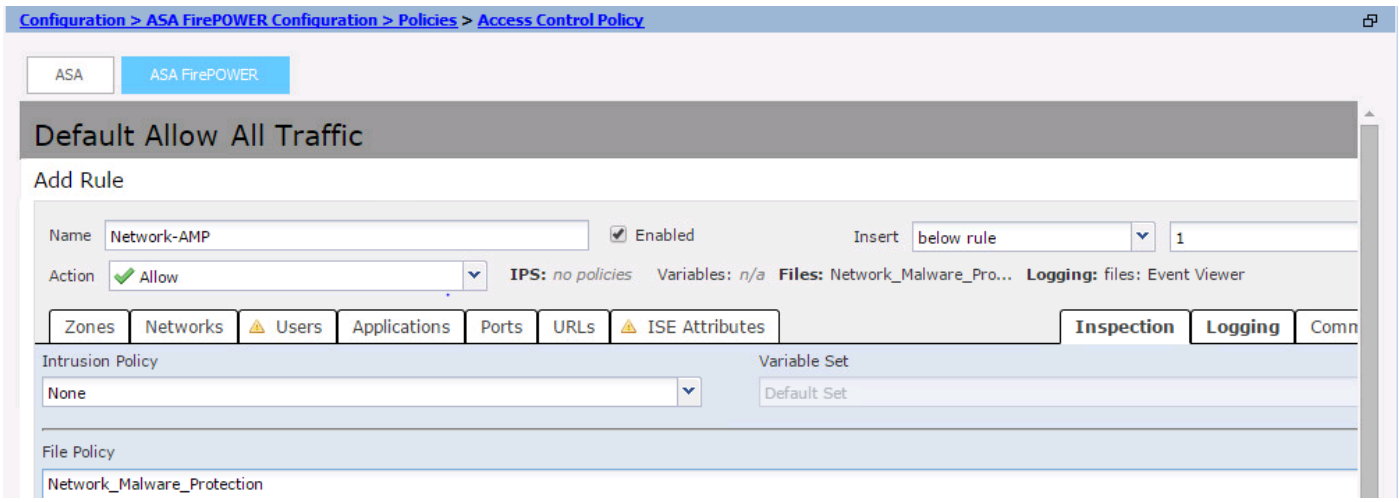
Configurez la stratégie de contrôle d'accès pour la stratégie de fichier

Naviguez vers la **configuration > la configuration ASA FirePOWER > les stratégies > la stratégie de contrôle d'accès,** et créez l'un ou l'autre de nouvelle **règle d'accès** ou éditez la règle d'accès existante**,** suivant les indications de cette image.

Pour configurer la stratégie de fichier, l'action devrait être **laissent**. Naviguez vers l'onglet d'**inspection**, et sélectionnez la **stratégie de fichier du** menu de baisse vers le bas.

Pour activer se connecter, naviguez l'option **se connectante**, et sélectionnez l'option se connectante appropriée et l'option de **fichiers journal**. Cliquez sur la **sauvegarde/ajoutez le** bouton pour sauvegarder la configuration.

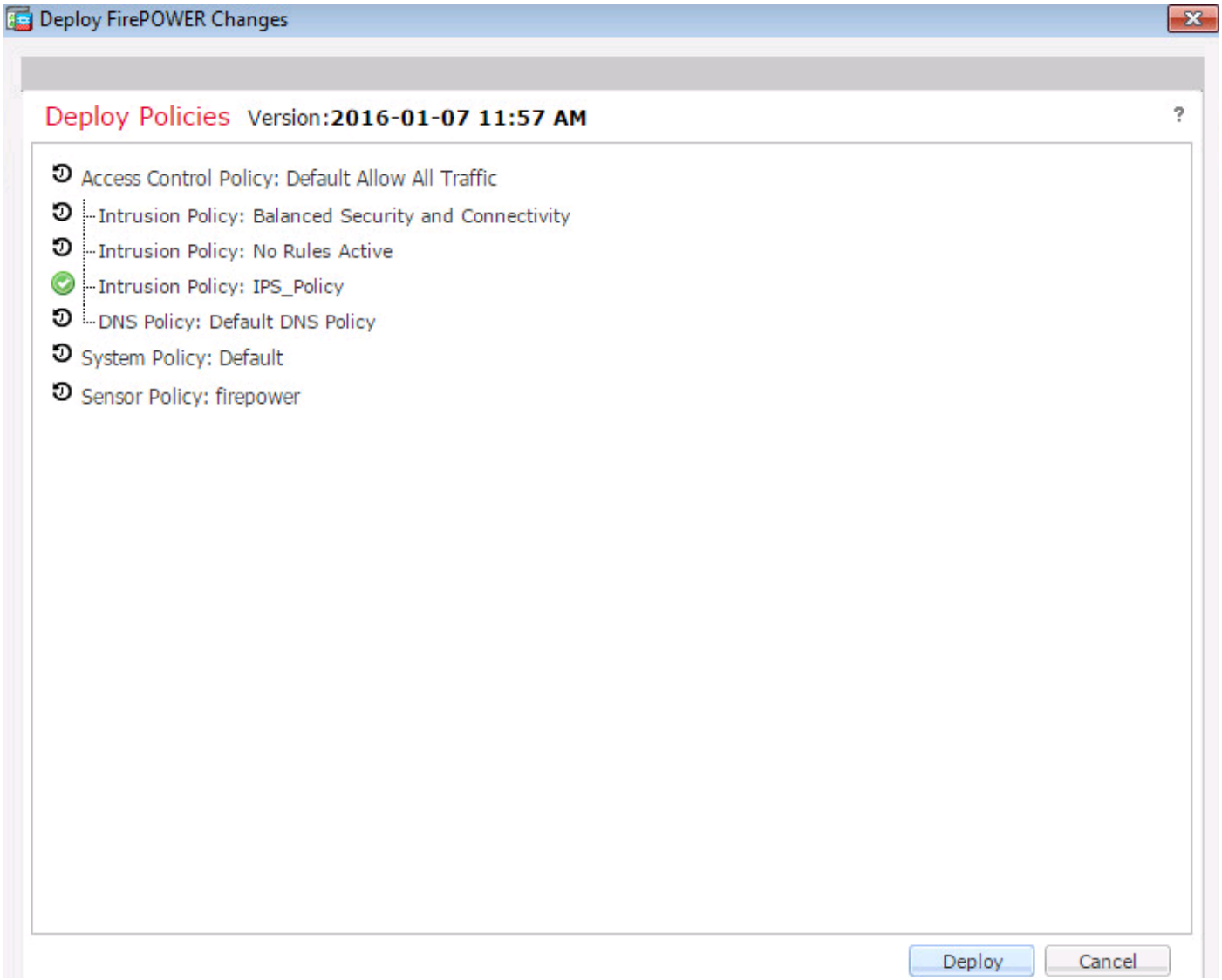
Choisissez les **modifications de la mémoire ASA FirePOWER d'**option pour sauvegarder les changements de politique à C.A.



Déployez la stratégie de contrôle d'accès

Naviguez vers des ASDM **déploient l'**option, et choisissent **déploient l'**option de **modification de FirePOWER du** menu de baisse vers le bas. Cliquez sur en fonction l'option **Deploy** de déployer

les modifications.

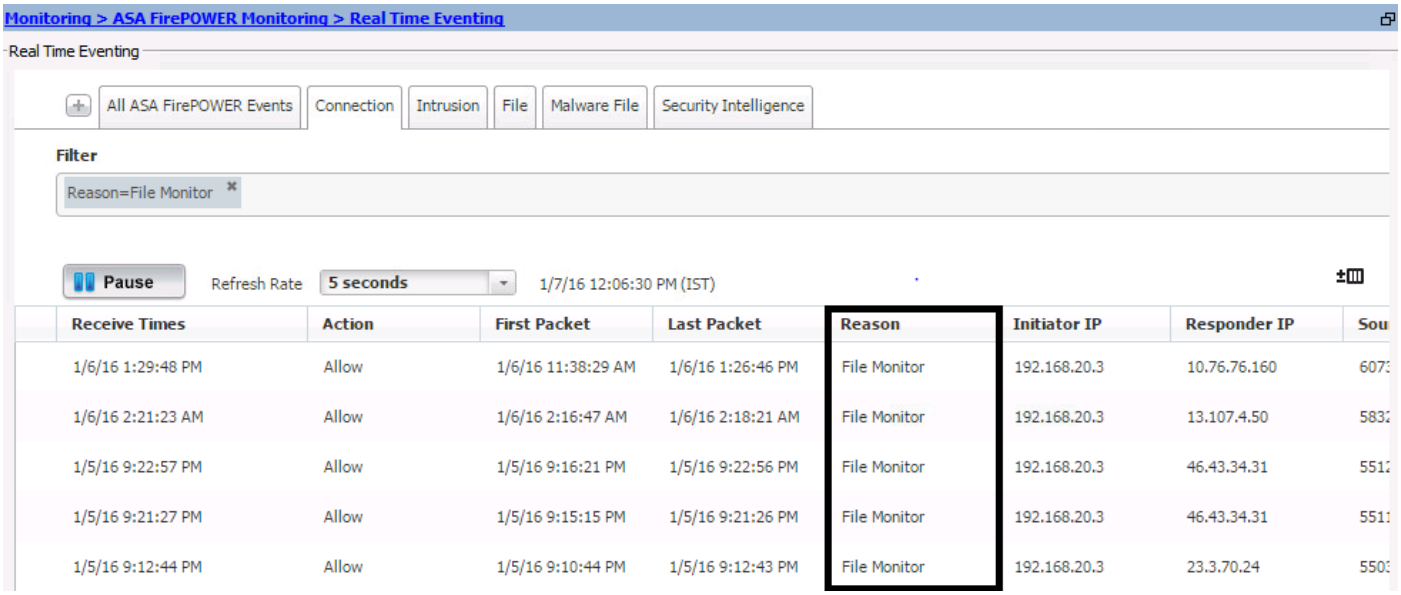


Naviguez vers la **surveillance > ASA FirePOWER surveillant > état de tâche.** Assurez-vous que la tâche doit se terminer pour appliquer la modification de configuration.

> **Note**: Dans la version 5.4.x, pour appliquer la stratégie d'accès au capteur, vous avez besoin clickApply des **modifications ASA FirePOWER.**

Surveillez la connexion pour des événements de stratégie de fichier

Afin de voir les événements générés par le module de FirePOWER rapporté pour classer la stratégie, naviguez vers la **surveillance > ASA FirePOWER surveillant > concours complet en temps réel.**



Vérifiez

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

Dépannez

Assurez-vous que la stratégie de fichier conifigured correctement avec des types de fichier d'action de direction de protocole. Assurez à cela la stratégie correcte de fichier incluse dans les règles d'accès.

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

Surveillez les événements de connexion et les événements de fichier (**surveillance > ASA FirePOWER surveillant > concours complet en temps réel**) pour vérifier si la circulation frappe la règle correcte ou pas.

Informations connexes

- Support et documentation techniques - Cisco Systems