

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](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Aperçu de flux de renseignements de sécurité](#)

[Ajoutez manuellement la Global-liste noire d'adresses IP et global-Whitelist](#)

[Créez la liste faite sur commande d'adresse IP de liste noire](#)

[Configurez les renseignements de sécurité](#)

[Déployez la stratégie de contrôle d'accès](#)

[Surveillance des événements des renseignements de sécurité](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

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 FirePOWER

Note: 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 ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) et en haut
- Version de logiciel courante 6.0.0 du module ASA FirePOWER (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 FirePOWER 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 FirePOWER 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 > ASA FirePOWER surveillant > 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.

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

+ All ASA FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter
Rule Action=Allow *

Pause Refresh Rate 5 seconds 1/25/16 9:11:25 AM (IST)

Receive Times	Action	First Packet	Last Packet	Reason
1/25/16 9:09:50 AM	Allow	1/25/16 9:09:48 AM	1/25/16 9:09:49 AM	
1/25/16 9:07:36 AM	Allow	1/25/16 9:07:03 AM	1/25/16 9:07:03 AM	
1/25/16 9:07:07 AM	Allow	1/25/16 9:07:06 AM	1/25/16 9:07:06 AM	

View details

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

Initiator	Responder	Edit
Initiator IP 192.168.20.3	Responder IP 10.106.44.55	
Initiator Country and Continent not available	Responder Country and Continent not available	
Source Port/ICMP Type 60297	Destination Port/ICMP 49153	

Whitelist Now
Blacklist Now

Afin de vérifier que la source ou l'adresse IP de destination est ajoutée au Global-Blacklist/global-Whitelist, naviguez vers la configuration > la configuration ASA FirePOWER > 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

FirePOWER 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 FirePOWER. Afin de télécharger le fichier, naviguez vers la configuration > la configuration ASA FirePOWER > 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 parcourir 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 FirePOWER contacte le serveur de tiers pour chercher la liste d'adresse IP. Afin de configurer ceci, naviguez vers la configuration > la

configuration ASA FirePOWER > 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 FirePOWER 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.

The image displays two screenshots of the ASA FirePOWER configuration interface, specifically the 'Security Intelligence for Network List / Feed' dialog box. The top screenshot shows the configuration for a 'List' type feed. The 'Name' field is set to 'Custom_Feed', the 'Type' is 'List', and the 'Upload List' field contains the path 'C:\fakepath\Custom_IP_Feed.'. The bottom screenshot shows the configuration for a 'Feed' type feed. The 'Name' field is set to 'Custom_Network_Feed', the 'Type' is 'Feed', the 'Feed URL' is 'http://192.168.30.1/blacklist-IP.txt', the 'MD5 URL' is '(optional)', and the 'Update Frequency' is set to '30 minutes'. Both screenshots show a list of existing feeds on the left, including 'Cisco-Intelligence-Feed', 'Custom_Feed', 'Global-Blacklist', and 'Global-Whitelist'. The interface includes buttons for 'Update Feeds', 'Add Network Lists and Feeds', 'Upload', 'Store ASA FirePOWER Changes', and 'Cancel'.

Configurez les renseignements de sécurité

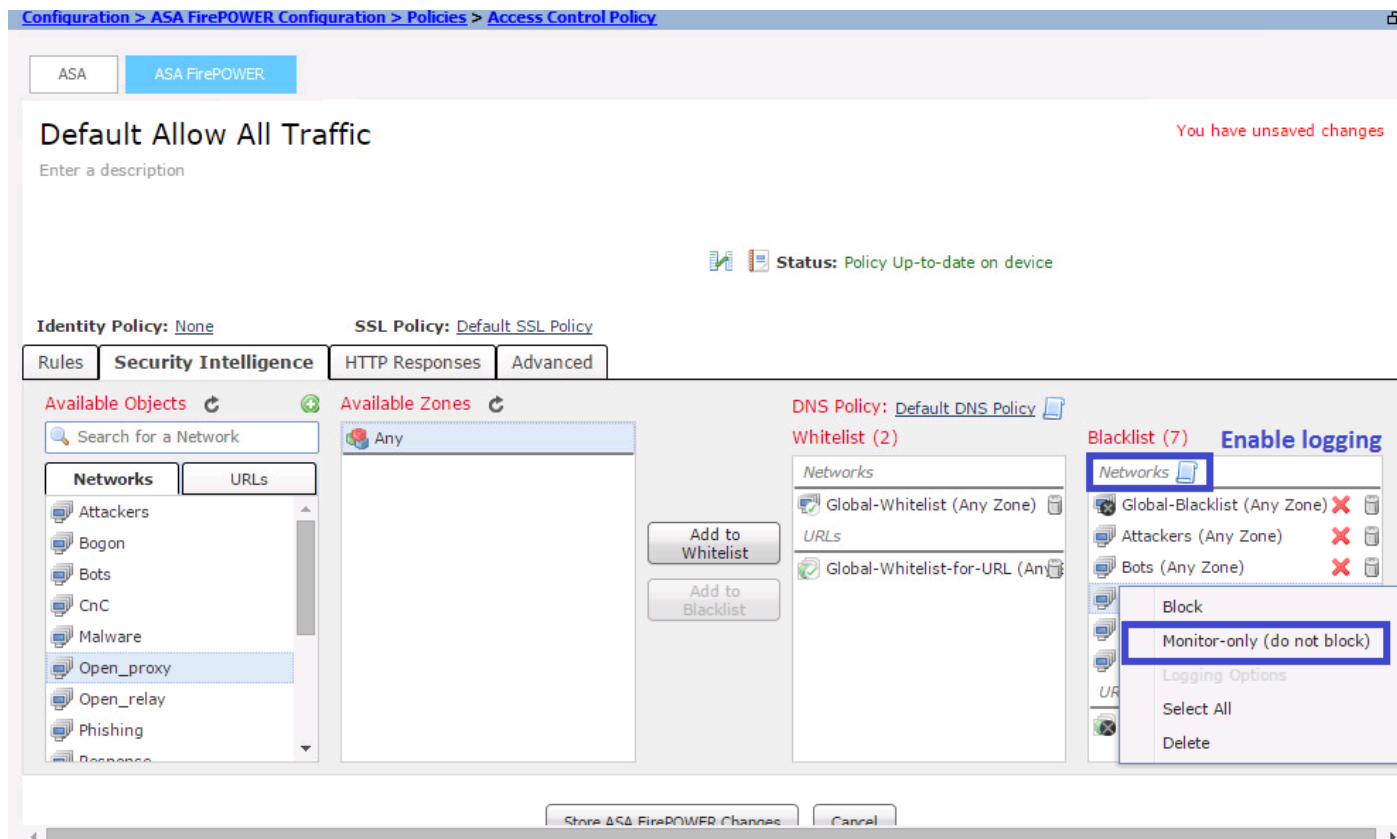
Afin de configurer des renseignements de sécurité, naviguez vers la configuration > la configuration ASA FirePOWER > les stratégies > la stratégie de contrôle d'accès, onglet choisi de

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, choisissez **réserver au moniteur (ne font pas le bloc)**, suivant les indications de l'image :

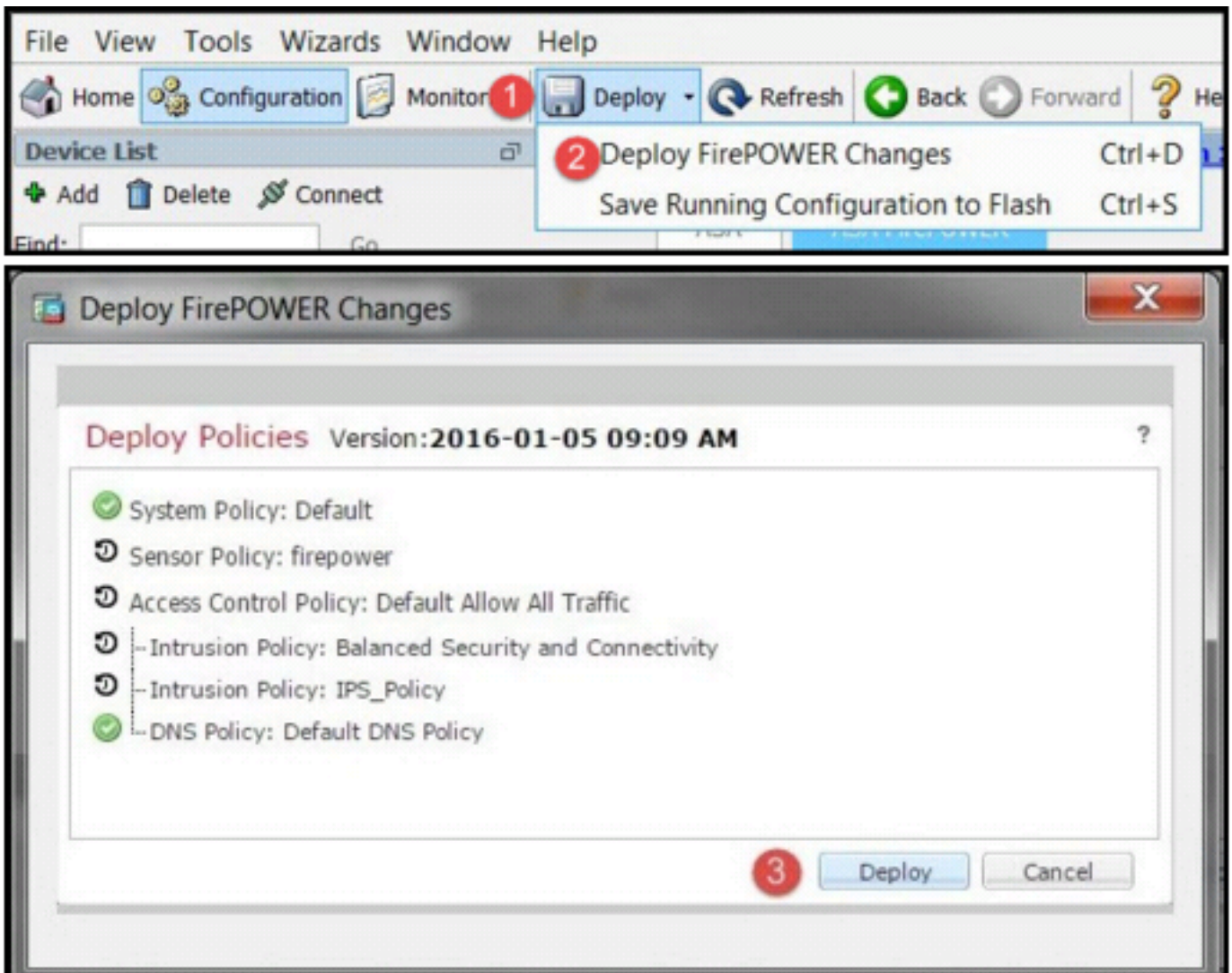


Choisissez les modifications de la mémoire ASA FirePOWER d'option pour sauvegarder les changements de politique à C.A.

Déployez la stratégie de contrôle d'accès

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 FirePOWER** puis les sélectionnent **se déploient** dans la fenêtre externe pour déployer les modifications.



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

Note: Naviguez vers la **surveillance > ASA FirePOWER surveillant > 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 FirePOWER, naviguez vers la **surveillance > ASA FirePOWER surveillant > concours complet en temps réel**. Sélectionnez l'onglet de **renseignements de sécurité**. Ceci révélera les événements suivant les indications de l'image :

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

All FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter

Enter filter criteria

Pause Refresh Rate 5 seconds 2/9/16 1:03:31 PM (IST)

Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP
2/9/16 1:01:48 PM	Block	2/9/16 1:01:47 PM		IP Block	192.168.20.3	184.26.162.43

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 > la configuration ASA FirePOWER > 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.

Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds

Update Feeds Add Network Lists and Feeds Filter

Name	Type	
Cisco-Intelligence-Feed <i>Last Updated: 2016-02-08 10:03:14</i>	Feed	 
Custom_Feed	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

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 Cisco ASA FirePOWER](#)
- [Support et documentation techniques - Cisco Systems](#)