

Configurer la mise en veille sur IP lors de l'utilisation de Cisco Security Intelligence via ASDM (gestion intégrée)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Présentation du flux Security Intelligence](#)

[Ajouter manuellement des adresses IP à la liste de blocage globale et à la liste d'autorisation globale](#)

[Créer une liste personnalisée d'adresses IP de liste noire](#)

[Configurer l'intelligence de sécurité](#)

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

[Surveillance des événements de Security Intelligence](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit la réputation de Cisco Security Intelligence/IP address et la configuration de la liste noire IP (Blocage) lors de l'utilisation d'un flux personnalisé/automatique d'adresse IP de faible réputation.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du pare-feu ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Connaissances de l'appliance FirePOWER

Note: Le filtrage Security Intelligence nécessite une licence Protection.

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 le logiciel version 5.4.1 et ultérieure
- Module ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) exécutant le logiciel version 6.0.0 et ultérieure

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Cisco Security Intelligence se compose de plusieurs ensembles d'adresses IP régulièrement mis à jour et dont la réputation est jugée médiocre par l'équipe Cisco TALOS. L'équipe Cisco TALOS détermine la faible réputation si une activité malveillante provient d'adresses IP telles que les spams, les programmes malveillants, les attaques d'hameçonnage, etc.

Le flux de données Cisco IP Security Intelligence suit la base de données des pirates, des bots, des bots, des CnC, des Dga, des ExploitKit, des programmes malveillants, des proxys ouverts, des relais ouverts, des tentatives d'hameçonnage, des réponses, des spams et des messages suspects. Le module Firepower offre la possibilité de créer le flux personnalisé d'adresse IP de faible réputation.

Présentation du flux Security Intelligence

Voici quelques informations supplémentaires sur le type de collections d'adresses IP qui peuvent être classées en différentes catégories dans Security Intelligence.

Les pirates : Ensemble d'adresses IP qui recherchent en permanence des vulnérabilités ou tentent d'exploiter d'autres systèmes.

Programme malveillant : Ensemble d'adresses IP qui tentent de propager des programmes malveillants ou attaquent activement quiconque les visite.

Hameçonnage : Collection d'hôtes qui tentent activement de tromper les utilisateurs finaux pour qu'ils saisissent des informations confidentielles telles que des noms d'utilisateur et des mots de passe.

Spam : Collection d'hôtes identifiés comme source d'envoi de courriers indésirables.

Bots : Collection d'hôtes qui participent activement dans le cadre d'un botnet et qui sont contrôlés par un contrôleur de réseau de robot connu.

CnC : Collection d'hôtes identifiés comme serveurs de contrôle pour un Botnet connu.

OpenProxy : Collection d'hôtes connus pour exécuter des serveurs proxy Web ouverts et offrir des services de navigation Web anonymes.

OpenRelay : Ensemble d'hôtes connus pour offrir des services de relais de messagerie anonyme

utilisés par les pirates de spam et d'hameçonnage.

TorExitNode : Ensemble d'hôtes connus pour offrir des services de noeud de sortie pour le réseau Tor Anonymizer.

Bogon : Collection d'adresses IP qui ne sont pas attribuées mais qui envoient du trafic.

Suspecte : Collection d'adresses IP affichant une activité suspecte et faisant l'objet d'une enquête active.

Réponse : Collection d'adresses IP qui ont été observées à plusieurs reprises et qui se sont livrées à un comportement suspect ou malveillant.

Ajouter manuellement des adresses IP à la liste de blocage globale et à la liste d'autorisation globale

Firepower vous permet d'ajouter certaines adresses IP à Global-Blacklist lorsque vous savez qu'elles font partie d'une activité malveillante. Les adresses IP peuvent également être ajoutées à la liste d'autorisation globale si vous voulez autoriser le trafic vers certaines adresses IP bloquées par des adresses IP de liste noire. Si vous ajoutez une adresse IP à Global-Blacklist/Global-Whitelist, elle prend effet immédiatement sans qu'il soit nécessaire d'appliquer la stratégie.

Afin d'ajouter l'adresse IP à Global-Blacklist/ Global-Whitelist, naviguez jusqu'à **Monitoring > ASA FirePOWER Monitoring > Real Time Event**, pointez la souris sur les événements de connexion et sélectionnez **View Details**.

Vous pouvez ajouter l'adresse IP source ou de destination à la liste globale de blocage/liste globale d'autorisation. Cliquez sur le bouton **Edit** et sélectionnez **Whitelist Now/Blacklist Now** pour ajouter l'adresse IP à la liste respective, comme illustré dans 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 l'adresse IP source ou de destination est ajoutée à la liste de blocage global/liste d'autorisation globale, accédez à **Configuration > ASA Firepower Configuration > Object Management > Security Intelligence > Network Lists and Feeds** et modifiez **Global-Blacklist/ Global Whitelist**. Vous pouvez également utiliser le bouton Supprimer pour supprimer toute adresse IP de la liste.

Créer une liste personnalisée d'adresses IP de liste noire

Firepower vous permet de créer une liste d'adresses réseau/IP personnalisée qui peut être utilisée dans la liste noire (blocage). Trois options s'offrent à vous :

1. Vous pouvez écrire les adresses IP dans un fichier texte (une adresse IP par ligne) et télécharger le fichier dans Firepower Module. Afin de télécharger le fichier, accédez à **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds**, puis cliquez sur **Add Network Lists and Feeds**
Name : Spécifiez le nom de la liste personnalisée. **type** : Sélectionnez **Liste** dans la liste déroulante. **Liste de téléchargement** : Choisissez **Parcourir** pour localiser le fichier texte dans votre système. Sélectionnez l'option **Télécharger** pour télécharger le fichier.
2. Vous pouvez utiliser n'importe quelle base de données IP tierce pour la liste personnalisée pour laquelle le module Firepower contacte le serveur tiers pour récupérer la liste d'adresses IP. Pour configurer ceci, accédez à **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds**, puis cliquez sur **Add**

Network Lists and Feeds

Name : Spécifiez le nom du flux personnalisé.

type : Sélectionnez l'option **Flux** dans la liste déroulante.

URL du flux : Spécifiez l'URL du serveur auquel le module Firepower doit se connecter et télécharger le flux.

URL MD5 : Spécifiez la valeur de hachage pour valider le chemin d'URL du flux.

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

The image displays two screenshots of the ASA FirePOWER configuration interface, specifically the 'Network Lists and Feeds' section. The top screenshot shows the configuration for a 'List' type feed named 'Custom_Feed'. The configuration fields are: Name: Custom_Feed, Type: List, Upload List: C:\fakepath\Custom_IP_Feed. The bottom screenshot shows the configuration for a 'Feed' type feed named 'Custom_Network_Feed'. The configuration fields are: Name: Custom_Network_Feed, Type: Feed, Feed URL: http://192.168.30.1/blacklist-IP.txt, MD5 URL: (optional), Update Frequency: 30 minutes. Both screenshots show a breadcrumb trail: Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds. The interface includes buttons for 'Update Feeds', 'Add Network Lists and Feeds', 'Upload', 'Store ASA FirePOWER Changes', and 'Cancel'. A table on the left lists existing feeds: Cisco-Intelligence-Feed (Last Updated: 2016-01-22 05:56:), Custom_Feed, Global-Blacklist, and Global-Whitelist.

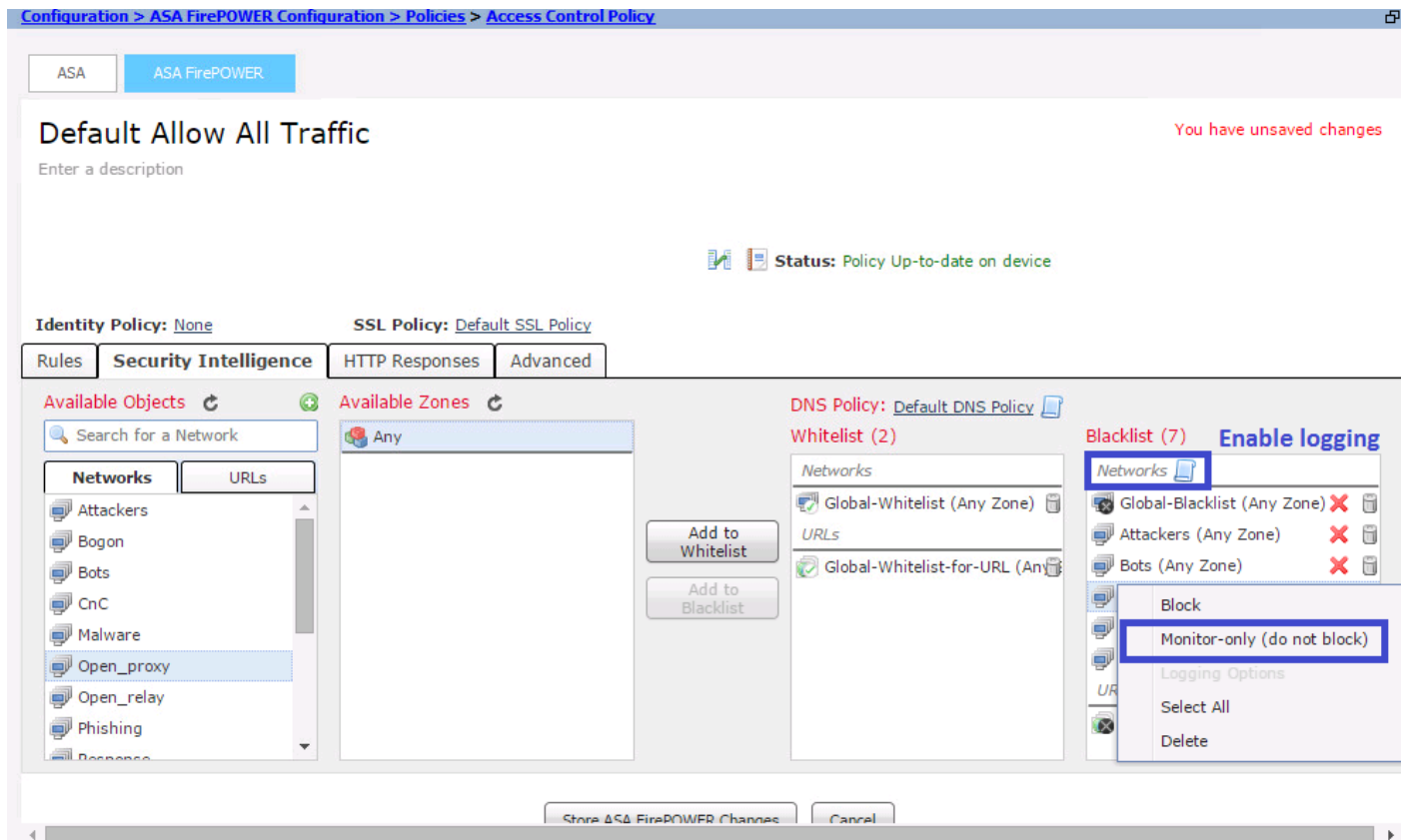
Configurer l'intelligence de sécurité

Afin de configurer Security Intelligence, accédez à **Configuration > ASA Firepower Configuration > Policies > Access Control Policy**, sélectionnez **Security Intelligence** tab.

Choisissez le flux dans l'objet Network Available, passez à la colonne **Liste blanche/Liste noire** pour autoriser/bloquer la connexion à l'adresse IP malveillante.

Vous pouvez cliquer sur l'icône et activer la journalisation comme indiqué dans l'image.

Si vous voulez simplement générer l'événement pour les connexions IP malveillantes au lieu de bloquer la connexion, cliquez avec le bouton droit sur le flux, choisissez **Surveillance uniquement (ne pas bloquer)**, comme indiqué dans l'image :

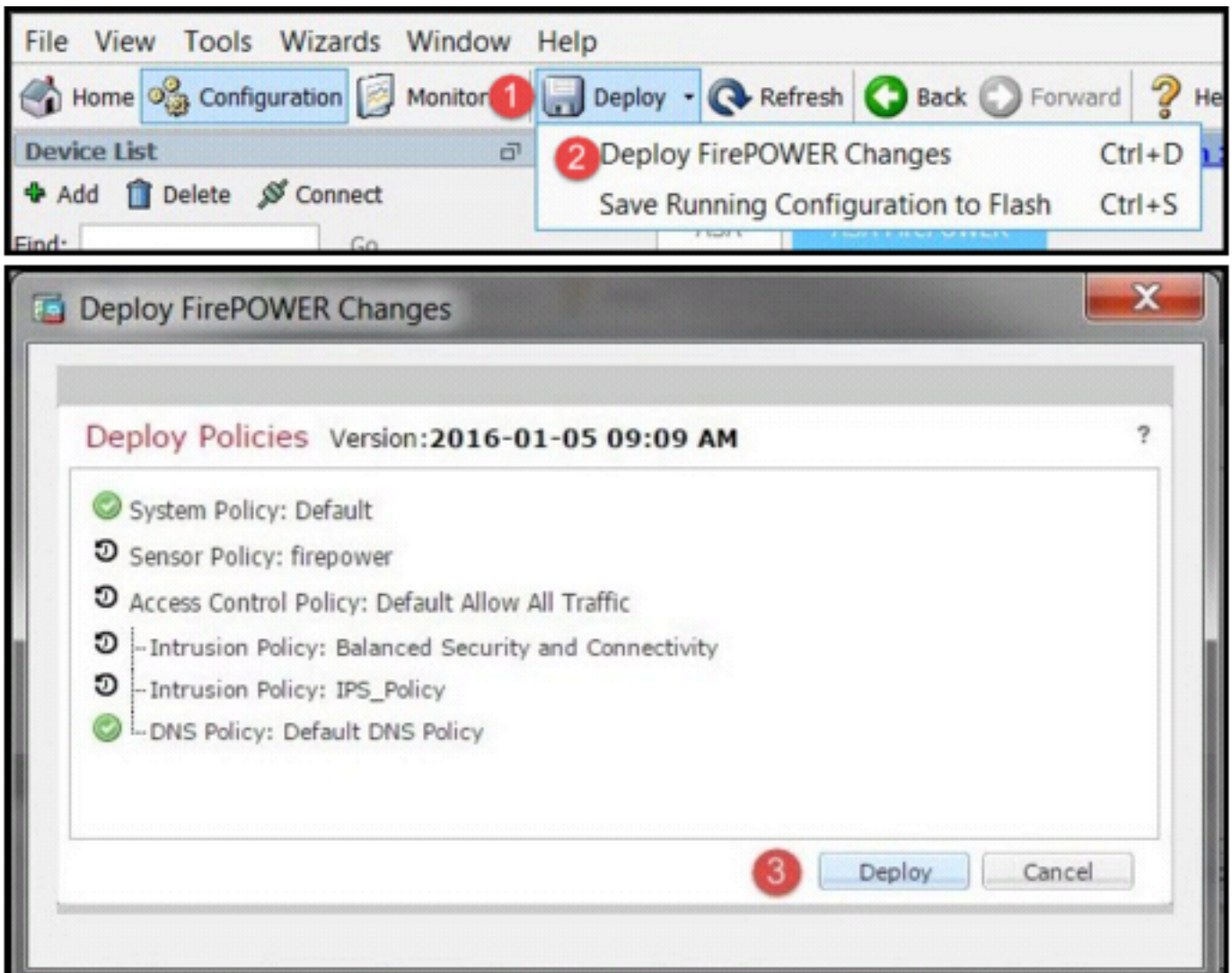


Sélectionnez l'option Store ASA Firepower Changes pour enregistrer les modifications de la stratégie CA.

Déployer la stratégie de contrôle d'accès

Pour que les modifications prennent effet, vous devez déployer la stratégie de contrôle d'accès. Avant d'appliquer la stratégie, vérifiez si la stratégie de contrôle d'accès est obsolète ou non sur le périphérique.

Pour déployer les modifications sur le capteur, cliquez sur **Déployer** et choisissez **Déployer les modifications FirePOWER** puis sélectionnez **Déployer** dans la fenêtre contextuelle pour déployer les modifications.



Remarque:: Dans la version 5.4.x, pour appliquer la stratégie d'accès au capteur, cliquez sur **Appliquer les modifications ASA FirePOWER**

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

Surveillance des événements de Security Intelligence

Afin de voir l'intelligence de sécurité par le module Firepower, accédez à **Monitoring > ASA Firepower Monitoring > Real Time Evant**. Sélectionnez l'onglet **Security Intelligence**. Les événements s'affichent comme illustré sur l'image :

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

All ASA 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

Vérification









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

Dépannage

Afin de vous assurer que Security Intelligence Feeds est à jour, accédez à **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** et vérifiez l'heure de la dernière mise à jour du flux. Vous pouvez cliquer sur le bouton Modifier pour définir la fréquence de mise à jour du 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 Last Updated: 2016-02-08 10:03:14	Feed	 
Custom_Feed	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

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

Surveillez les informations de sécurité pour voir si le trafic est bloqué ou non.

Informations connexes

- [Guide de démarrage rapide du module Cisco ASA FirePOWER](#)
- [Support et documentation techniques - Cisco Systems](#)