

Exemple de configuration du filtrage des URL sur un système FireSIGHT

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Licence de filtrage d'URL requise](#)

[Configuration des ports](#)

[Components Used](#)

[Configuration](#)

[Activer le filtrage des URL sur FireSIGHT Management Center](#)

[Application d'une licence de filtrage URL sur un périphérique géré](#)

[Exclusion d'un site spécifique de la catégorie d'URL bloquée](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes pour configurer le filtrage des URL sur FireSIGHT System. La fonctionnalité de filtrage des URL de FireSIGHT Management Center vous permet d'écrire une condition dans une règle de contrôle d'accès afin de déterminer le trafic qui traverse un réseau en fonction des requêtes d'URL non chiffrées des hôtes surveillés.

Conditions préalables

Conditions requises

Ce document a quelques exigences spécifiques pour la licence de filtrage d'URL et le port.

Licence de filtrage d'URL requise

FireSIGHT Management Center nécessite une licence de filtrage des URL pour pouvoir contacter régulièrement le cloud afin d'obtenir des informations actualisées sur les URL. Vous pouvez ajouter des conditions d'URL basées sur la catégorie et la réputation aux règles de contrôle d'accès sans licence de filtrage d'URL ; toutefois, vous ne pouvez pas appliquer la stratégie de contrôle d'accès tant que vous n'avez pas ajouté une licence de filtrage des URL à FireSIGHT Management Center, puis l'avez activée sur les périphériques ciblés par la stratégie.

Si une licence de filtrage d'URL expire, les règles de contrôle d'accès avec des conditions d'URL basées sur la catégorie et la réputation arrêtent le filtrage des URL et FireSIGHT Management Center ne contacte plus le service cloud. Sans licence de filtrage d'URL, des URL individuelles ou des groupes d'URL peuvent être définis pour autoriser ou bloquer, mais la catégorie d'URL ou les

données de réputation ne peuvent pas être utilisées pour filtrer le trafic réseau.

Configuration des ports

Un système FireSIGHT utilise les ports 443/HTTPS et 80/HTTP pour communiquer avec le service cloud. Le port 443/HTTPS doit être ouvert de manière bidirectionnelle et l'accès entrant au port 80/HTTP doit être autorisé sur FireSIGHT Management Center.

Components Used

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

- Appliances FirePOWER : Gammes 7000, 8000
- Appareil virtuel NGIPS (Intrusion Prevention System) de nouvelle génération
- Appareil de sécurité adaptatif (ASA) FirePOWER
- Logiciel Sourcefire version 5.2 ou 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.

Configuration

Activer le filtrage des URL sur FireSIGHT Management Center

Pour activer le filtrage des URL, procédez comme suit :

1. Connectez-vous à l'interface utilisateur Web de FireSIGHT Management Center.
2. La navigation est différente en fonction de la version du logiciel que vous exécutez :

Dans la version 6.1.x, choisissez **System > Integration > Cisco CSI**.

Dans la version 5.x, choisissez **System > Local > Configuration**. Choisissez **Cloud Services**.

3. Cochez la case **Enable URL Filtering** afin d'activer le filtrage d'URL.
4. Vous pouvez également cocher la case **Enable Automatic Updates** afin d'activer les mises à jour automatiques. Cette option permet au système de contacter le service cloud régulièrement afin d'obtenir des mises à jour des données URL dans les ensembles de données locaux de l'appliance.

Note: Bien que le service cloud mette généralement à jour ses données une fois par jour, si vous activez les mises à jour automatiques, il force FireSIGHT Management Center à vérifier toutes les 30 minutes afin de s'assurer que les informations sont toujours à jour. Bien que les mises à jour quotidiennes soient généralement faibles, si plus de cinq jours se sont écoulés depuis la dernière mise à jour, le téléchargement des nouvelles données de filtrage d'URL peut prendre jusqu'à 20 minutes. Une fois les mises à jour téléchargées, l'exécution de la mise à jour peut prendre jusqu'à 30 minutes.

5. Vous pouvez également cocher la case **Interroger le cloud pour les URL inconnues** pour les URL inconnues afin d'interroger le service cloud pour les URL inconnues. Cette option permet au système d'interroger le cloud Sourcefire lorsqu'une personne de votre réseau

surveillé tente de rechercher une URL qui ne figure pas dans l'ensemble de données local. Si le cloud ne connaît pas la catégorie ou la réputation d'une URL, ou si FireSIGHT Management Center ne peut pas contacter le cloud, l'URL ne correspond pas aux règles de contrôle d'accès avec les conditions d'URL basées sur la catégorie ou la réputation.


Note: Vous ne pouvez pas attribuer manuellement des catégories ou des réputations aux URL. Désactivez cette option si vous ne souhaitez pas que vos URL non classées soient cataloguées par le cloud Sourcefire, par exemple, pour des raisons de confidentialité.

6. Cliquez sur **Save**. Les paramètres de filtrage des URL sont enregistrés.

Note: En fonction de la durée écoulée depuis la dernière activation du filtrage d'URL ou si c'est la première fois que vous activez le filtrage d'URL, FireSIGHT Management Center extrait les données de filtrage d'URL du service cloud.

Application d'une licence de filtrage URL sur un périphérique géré

1. Vérifiez si la licence de filtrage des URL est installée sur FireSIGHT Management Center. Accédez à la page **System > Licenses** afin de trouver une liste de licences.



The screenshot shows the 'Licenses' page in the FireSIGHT Management Center. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Licenses' tab is active. A table displays the license usage for various features:

Maximum Virtual Device 64bit Licenses	
Protection (Used)	1 (1)
Control (Used)	1 (1)
URL Filtering (Used)	1 (1)
Malware (Used)	1 (1)
VPN (Used)	0 (0)

2. Accédez à la page **Devices > Device Management** et vérifiez si la licence de filtrage d'URL est appliquée sur le périphérique qui surveille le trafic.



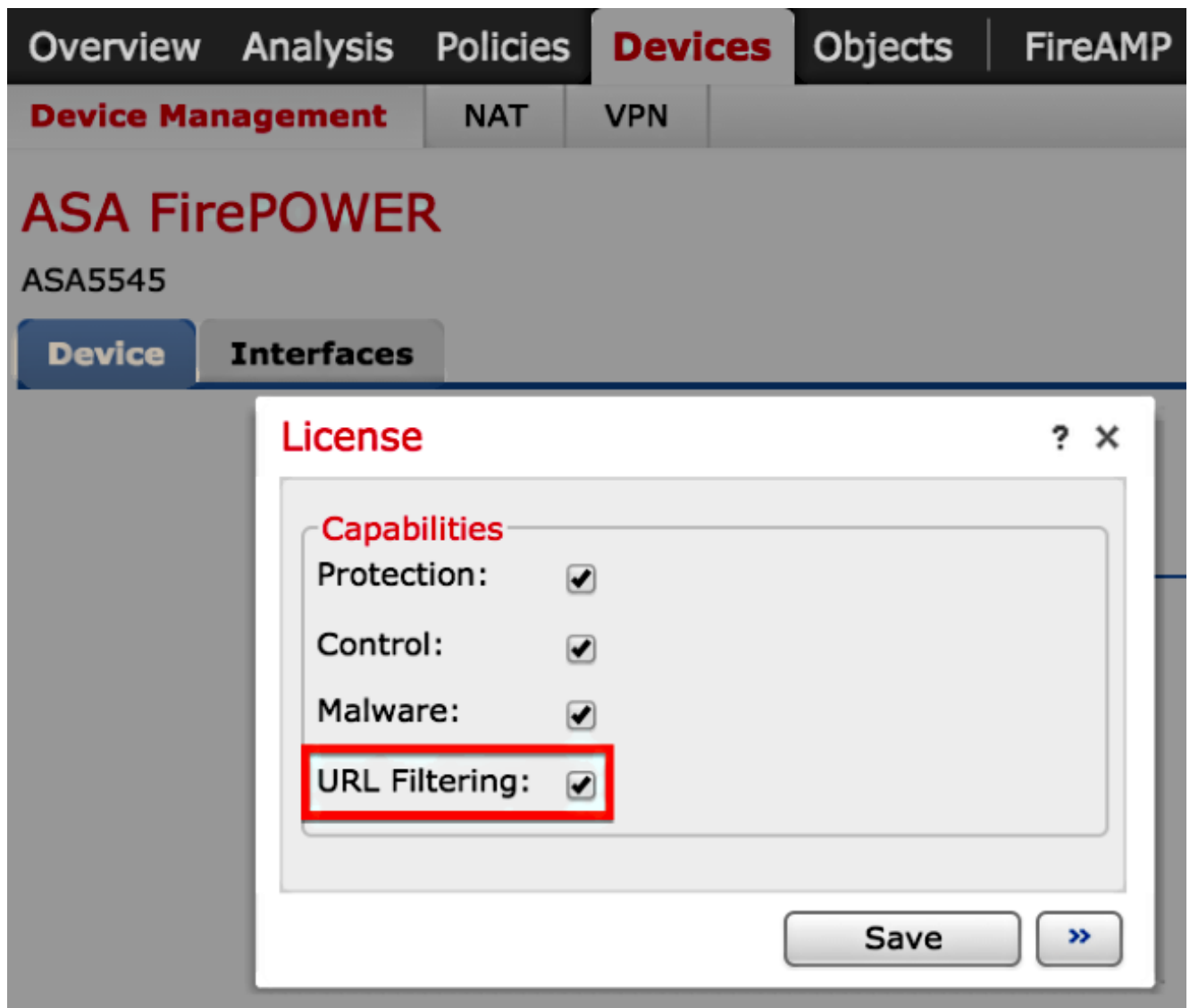
The screenshot shows the 'Device Management' page in the FireSIGHT Management Center. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Device Management' tab is active. A table displays the license information for a device:

Name	License Type	Health Policy
FirePOWER (1)		
ASA FirePOWER ASA5545 - v5.3.1	Protection, Control, Malware, URL Filtering	Initial Health Policy

3. Si la licence de filtrage d'URL n'est pas appliquée sur un périphérique, cliquez sur l'icône de **crayon** afin de modifier les paramètres. L'icône est située à côté du nom du périphérique.



4. Vous pouvez activer la licence de filtrage URL sur un périphérique à partir de l'onglet Périphériques.



5. Après avoir activé une licence et enregistré vos modifications, vous devez également cliquer sur **Apply Changes** afin d'appliquer la licence sur votre périphérique géré.

 **You have unapplied changes**



Exclusion d'un site spécifique de la catégorie d'URL bloquée

FireSIGHT Management Center ne vous permet pas d'avoir une évaluation locale des URL qui remplacent les évaluations de catégorie par défaut fournies par Sourcefire. Pour accomplir cette tâche, vous devez utiliser une stratégie de contrôle d'accès. Ces instructions décrivent comment utiliser un objet URL dans une règle de contrôle d'accès afin d'exclure un site spécifique d'une catégorie de bloc.

1. Accédez à la page **Objets > Gestion des objets**.

2. Choisissez **Objets individuels** pour l'URL, puis cliquez sur le bouton **Ajouter une URL**. La fenêtre **URL Objects** s'affiche.

URL Objects



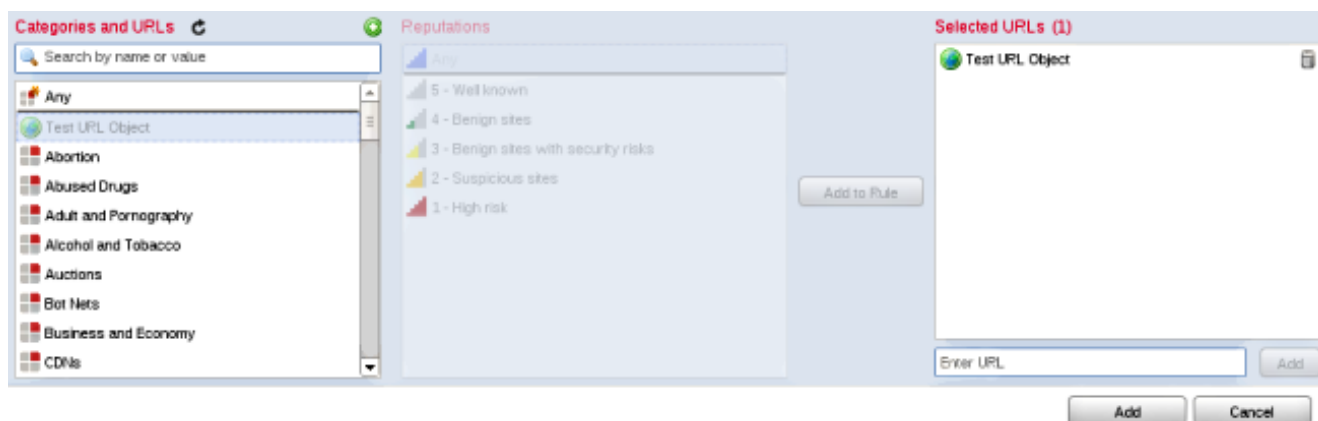
Name:	<input type="text" value="Test URL Object"/>
URL:	<input type="text" value="http://www.cisco.com"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Overview Analysis Policies Devices **Objects** FireAMP

Object Management

Name	Value
Test URL Object	http://www.cisco.com

3. Après avoir enregistré les modifications, choisissez **Policies > Access Control** et cliquez sur l'icône **crayon** afin de modifier la stratégie de contrôle d'accès.
4. Cliquez sur **Ajouter une règle**.
5. Ajoutez votre objet URL à la règle avec l'action **Autoriser** et placez-le au-dessus de la règle Catégorie d'URL, afin que son action de règle soit évaluée en premier.



6. Après avoir ajouté la règle, cliquez sur **Enregistrer et appliquer**. Il enregistre les nouvelles modifications et applique la stratégie de contrôle d'accès aux appareils gérés.

Vérification

Pour obtenir des informations sur la vérification ou le dépannage, reportez-vous à l'article **Troubleshoot Issues with URL Filtering on FireSIGHT System** lié à la section Related Information.

Dépannage

Pour obtenir des informations sur la vérification ou le dépannage, reportez-vous à la **Résolution des problèmes de filtrage des URL sur FireSIGHT System** article lié dans la section Informations connexes.

Informations connexes

- [Résolution des problèmes de filtrage des URL sur FireSIGHT System](#)
- [Support et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.