Filtrage URL sur un exemple de configuration système de FireSIGHT

Contenu

Introduction

Ce document décrit les étapes pour configurer le Filtrage URL sur le système de FireSIGHT. La caractéristique de Filtrage URL au centre de Gestion de FireSIGHT te permet pour écrire une condition dans une règle de contrôle d'accès afin de déterminer le trafic qui traverse un réseau basé sur des demandes non chiffrées URL par les hôtes surveillés.

Conditions préalables

Conditions requises

Ce document a quelques quelques conditions requises spécifiques pour le permis de Filtrage URL et le port.

Condition requise de permis de Filtrage URL

Un centre de Gestion de FireSIGHT exige d'un permis de Filtrage URL afin d'entrer en contact avec le nuage périodiquement pour une mise à jour sur les informations URL. Vous pouvez ajouter la catégorie et les conditions basées sur réputation URL aux règles de contrôle d'accès sans Filtrage URL autorisent ; toutefois vous ne pouvez pas appliquer la stratégie de contrôle d'accès jusqu'à ce que vous ajoutiez d'abord un permis de Filtrage URL au centre de Gestion de FireSIGHT, puis activez-le sur les périphériques visés par la stratégie.

Si un permis de Filtrage URL expire, le contrôle d'accès ordonne avec la catégorie et les états basés sur réputation URL cessent de filtrer l'URLs, et le centre de Gestion de FireSIGHT ne contacte plus le service en nuage. Sans permis de Filtrage URL, l'URLs individuel ou les groupes

d'URLs peut être placé pour laisser ou bloquer, mais les données de catégorie ou de réputation URL ne peuvent pas être utilisées afin de filtrer le trafic réseau.

Condition requise de port

Un système de FireSIGHT emploie les ports 443/HTTPS et 80/HTTP afin de communiquer avec le service en nuage. Le port 443/HTTPS doit être ouvert bidirectionnel, et on doit permettre l'accès entrant pour mettre en communication 80/HTTP au centre de Gestion de FireSIGHT.

Composants utilisés

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

- Appliances de FirePOWER : Gamme 7000, gamme 8000
- Appliance virtuelle du système de prévention des intrusions de nouvelle génération (NGIPS)
- Appliance de sécurité adaptable (ASA) FirePOWER
- Version de logiciel 5.2 de Sourcefire ou 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.

Configurez

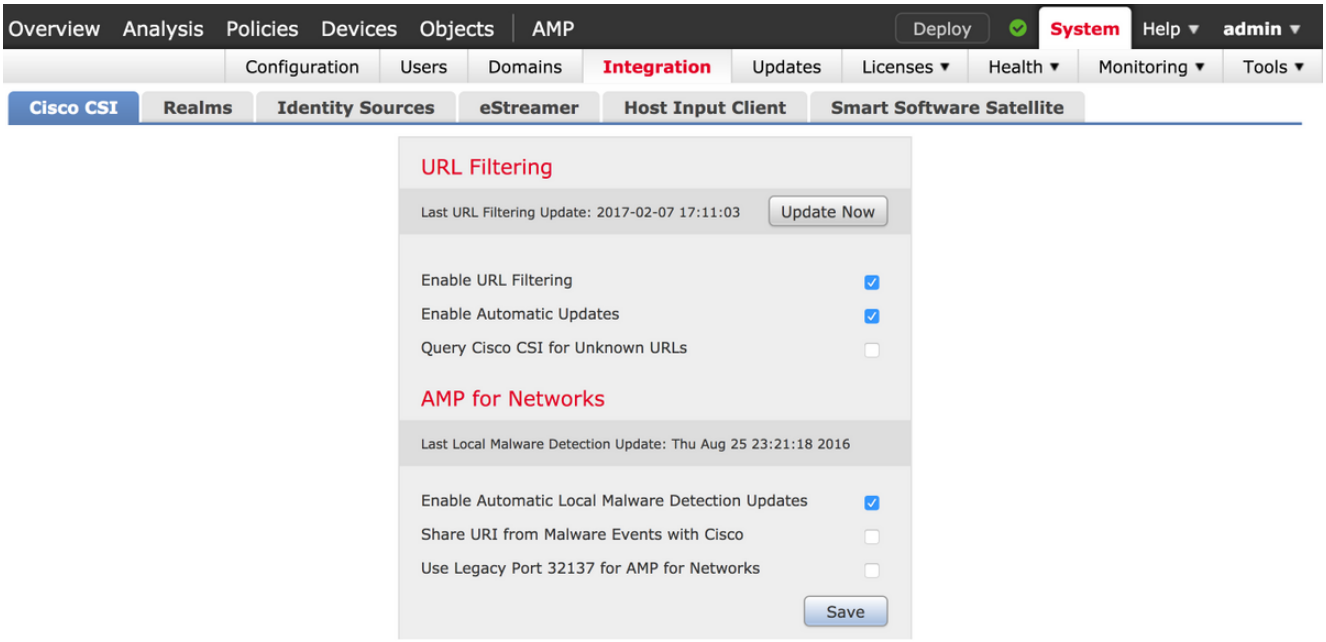
Filtrage URL d'enable au centre de Gestion de FireSIGHT

Afin d'activer le Filtrage URL, terminez-vous ces étapes :

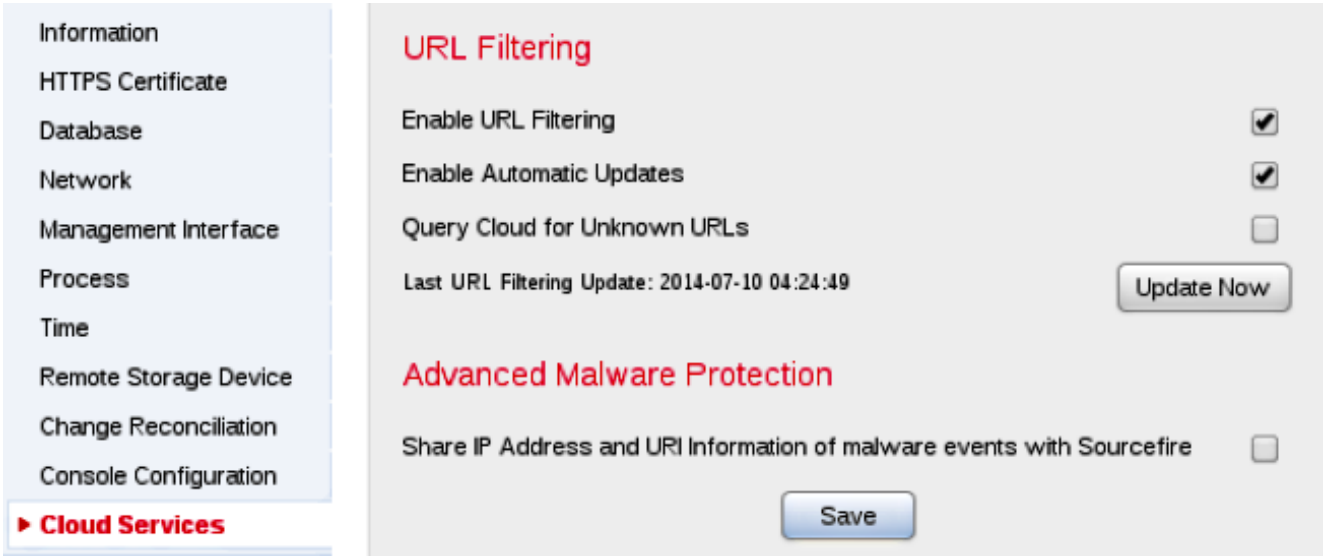
1. Connectez-vous dans l'interface utilisateur d'utilisateur web du centre de Gestion de FireSIGHT.

2. La navigation différent est basée sur la version de logiciel cette vous s'exécutent :

   Sur la version 6.1.x, choisissez le **système > l'intégration > le Cisco CSI**.



Sur la version 5.x, choisissez le **système > les gens du pays > la configuration**. Choisissez les **services en nuage**.



3. Cochez la case de **Filtrage URL d'enable** afin d'activer le Filtrage URL.
4. Sur option, cochez la case **automatique de mises à jour d'enable** afin d'activer les mises à jour automatiques. Cette option permet au système pour contacter le service en nuage de façon régulière afin d'obtenir des mises à jour aux données URL dans les postes de données locaux des appareils.

   Note: Bien que le service en nuage mette à jour typiquement ses données une fois par jour, si vous activez automatique le met à jour force le centre de Gestion de FireSIGHT pour vérifier toutes les 30 minutes afin de s'assurer que les informations sont toujours en cours. Bien que les mises à jour quotidiennes tendent à être petites, s'il a été plus de cinq jours depuis la dernière modification, les nouvelles données de Filtrage URL pourraient prendre à 20 minutes pour les télécharger. Une fois que les mises à jour ont été téléchargées, il pourrait prendre à 30 minutes pour exécuter la mise à jour elle-même.

5. Sur option, cochez le **nuage de requête pour l'URLs inconnu** pour la case inconnue URLs afin de questionner le service en nuage pour l'URLs inconnu. Cette option permet au

système pour questionner le nuage de Sourcefire quand quelqu'un sur vos tentatives surveillées de réseau de parcourir à un URL qui n'est pas dans le poste de données local. Si le nuage ne connaît pas la catégorie ou la réputation d'un URL, ou si le centre de Gestion de FireSIGHT ne peut pas entrer en contact avec le nuage, l'URL n'apparie pas des règles de contrôle d'accès avec la catégorie ou les états basés sur réputation URL.

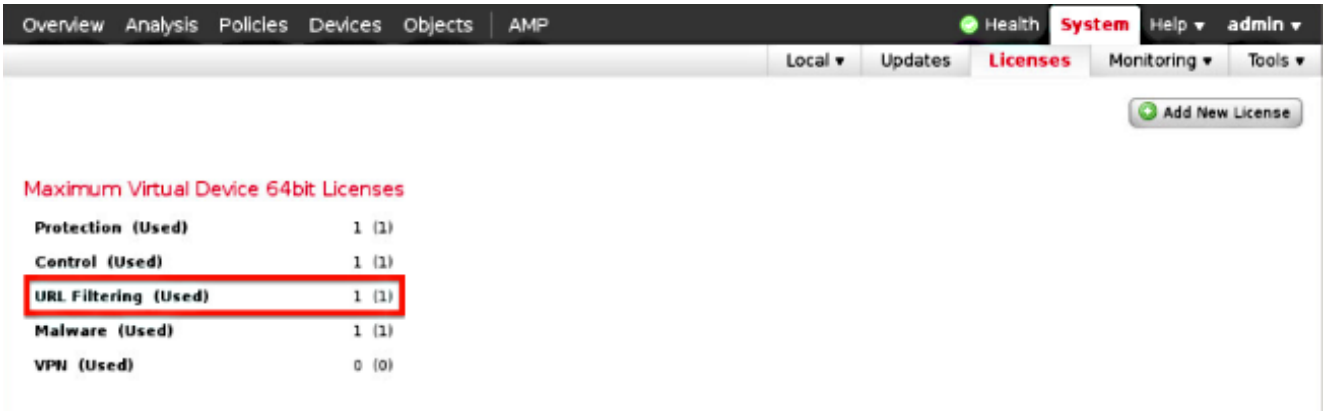
Note: Vous ne pouvez pas assigner des catégories ou des réputations à l'URLs manuellement. Désactivez cette option si vous ne voulez pas que votre URLs uncategorized soit catalogué par le nuage de Sourcefire, par exemple, pour des raisons d'intimité.

6. Cliquez sur **Save**. Des configurations de Filtrage URL sont enregistrées.

Note: Basé sur la durée puisque le Filtrage URL a été pour la dernière fois activé, ou si c'est la première fois vous ont activé le Filtrage URL, un centre de Gestion de FireSIGHT récupère les données de Filtrage URL du service en nuage.

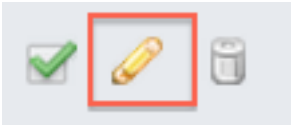
Appliquez le permis de Filtrage URL sur un périphérique géré

1. Vérifiez si le permis de Filtrage URL est installé au centre de Gestion de FireSIGHT. Allez à la page de **système > de permis** afin de trouver une liste de permis.

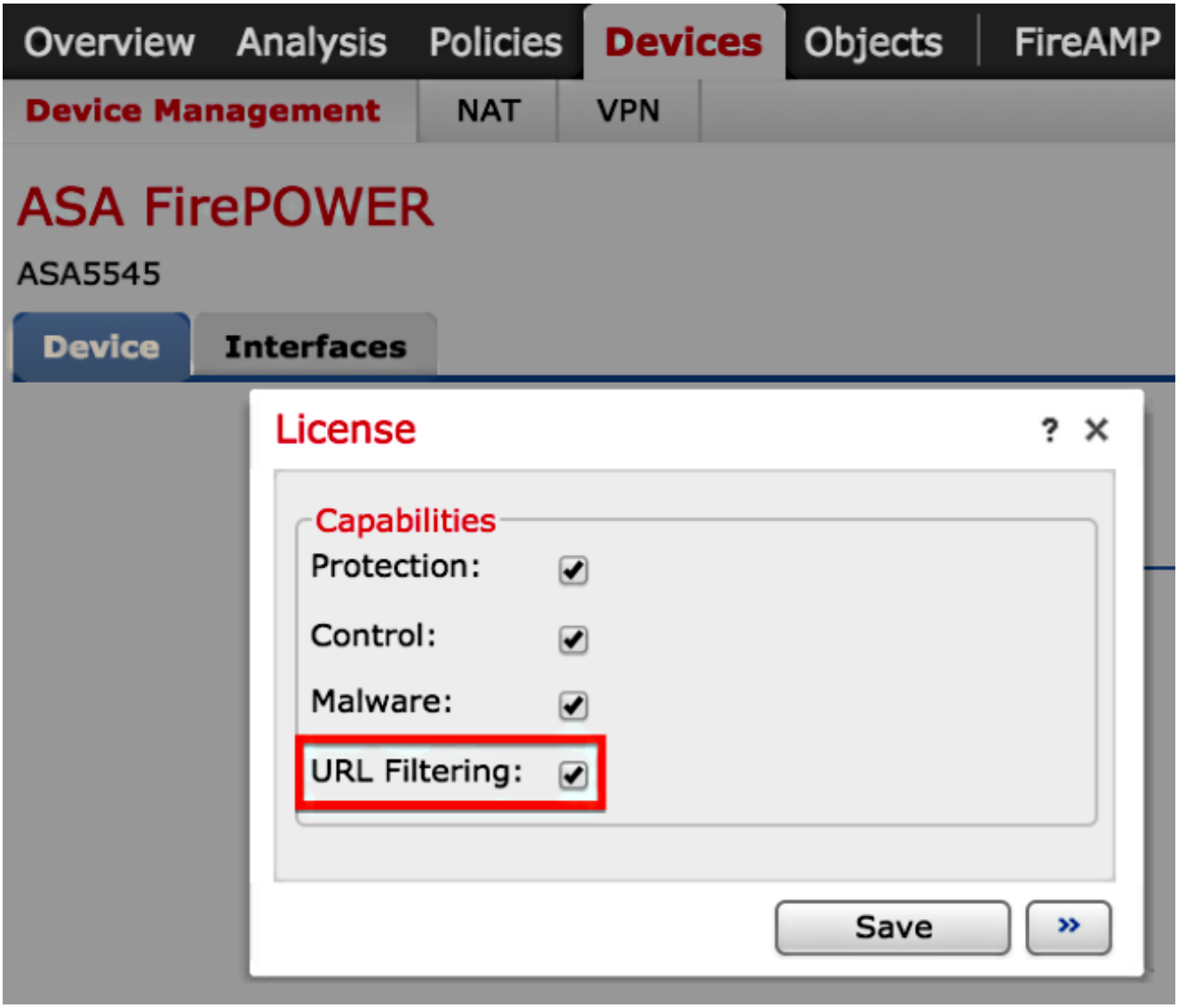


2. Allez à la page de **périphériques > de Gestion de périphériques**, et vérifiez si le permis de Filtrage URL est appliqué sur le périphérique qui surveille le trafic.

3. Si le permis de Filtrage URL n'est pas appliqué sur un périphérique, cliquez sur l'icône de **crayon** afin d'éditer les configurations. L'icône se trouve à côté du nom du périphérique.



4. Vous pouvez activer le permis de Filtrage URL sur un périphérique de l'onglet de **périphériques**.



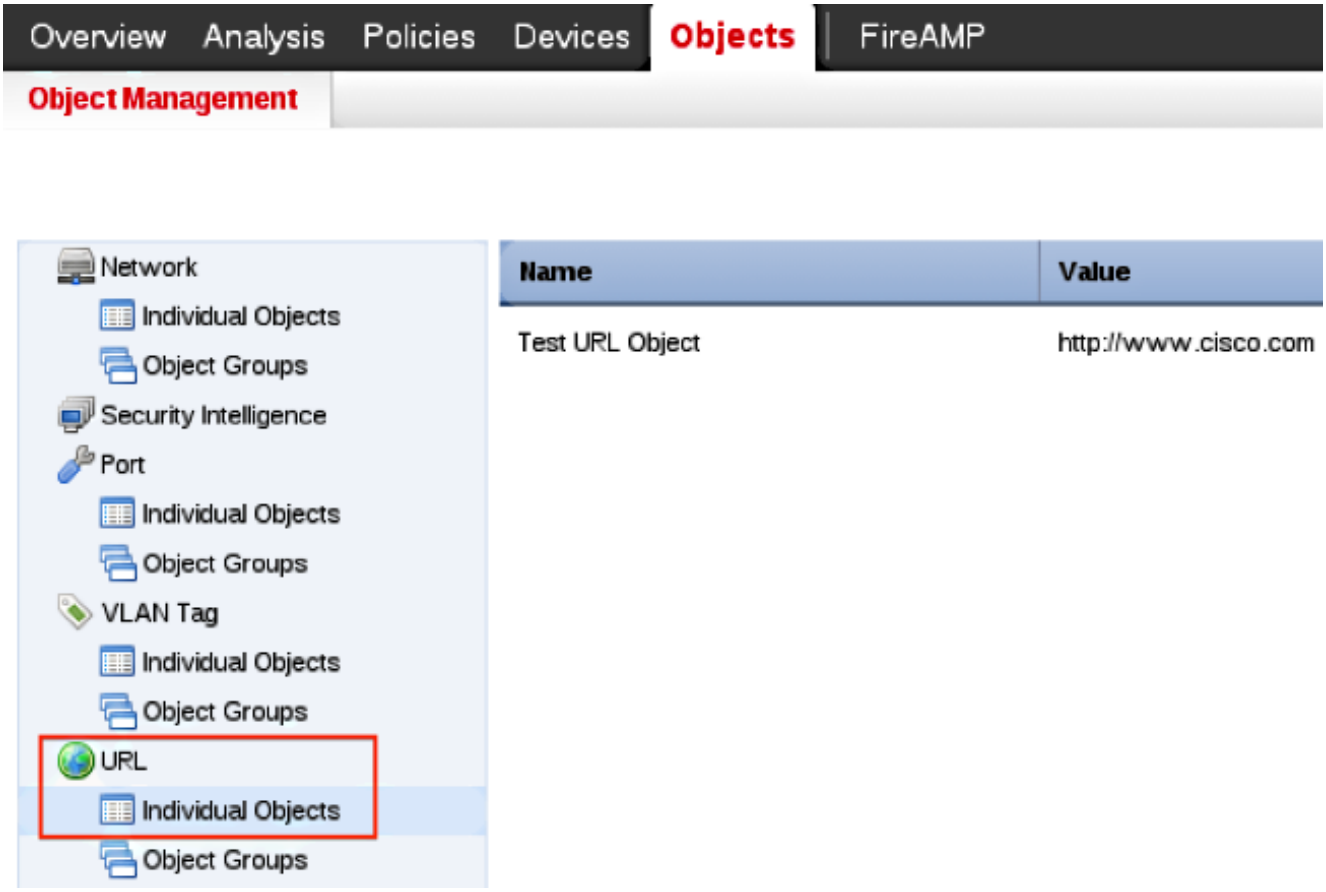
5. Après que vous activiez un permis et sauvegardiez vos modifications, vous devez également cliquer sur Apply des **modifications** afin d'appliquer le permis sur votre périphérique géré.

Exclusion d'un site spécifique de catégorie bloquée URL

Le centre de Gestion de FireSIGHT ne te permet pas pour avoir une évaluation locale d'URLs qui ignorent les évaluations par défaut de catégorie fournies par Sourcefire. Afin d'accomplir cette tâche, vous devez utiliser une stratégie de contrôle d'accès. Ces instructions décrivent comment employer un objet URL dans une règle de contrôle d'accès afin d'exclure un site spécifique d'une catégorie de bloc.

1. Allez aux **objets > à la** page de **Gestion d'objet**.

2. **Choisissez les différents objets** pour l'URL, et cliquez sur le bouton **URL d'ajouter**. La fenêtre d'**objets URL** apparaît.

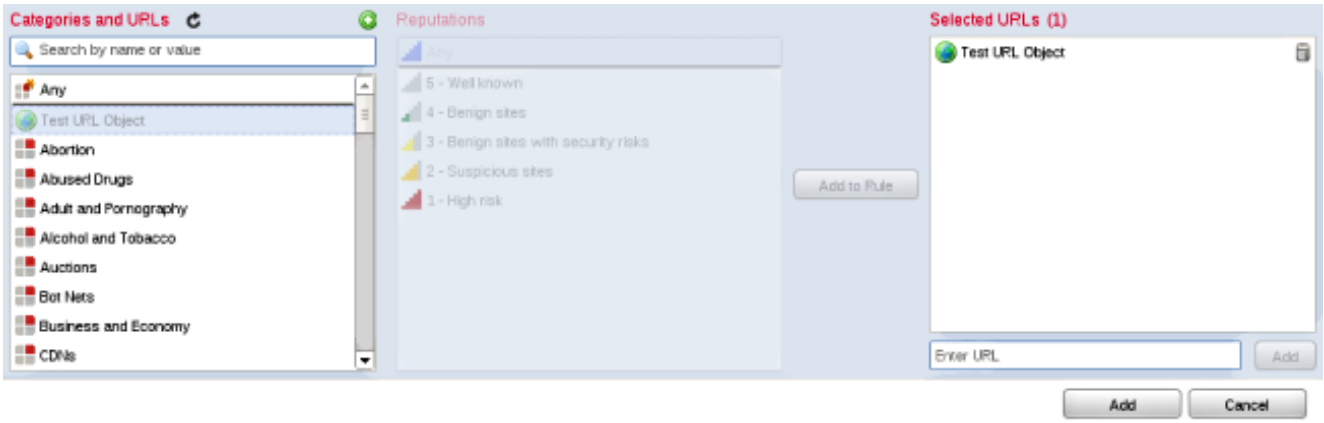


3. Après que vous sauvegardiez les modifications, choisissez les **stratégies > le contrôle d'accès** et cliquez sur l'icône de **crayon** afin d'éditer la stratégie de contrôle d'accès.

4. Cliquez sur Add la **règle**.

5. Ajoutez votre objet URL à la règle avec l'action d'**autoriser** et placez-le au-dessus de la règle

de catégorie URL, de sorte que son action de règle soit évaluée d'abord.



6. Après que vous ajoutiez la règle, cliquez sur la **sauvegarde et appliquez**. Il enregistre les nouvelles modifications et s'applique la stratégie de contrôle d'accès aux appliances gérées.

Vérifiez

Pour les informations Verify ou Troubleshoot, référez-vous aux **questions de dépannage avec le Filtrage URL sur l'**article de **système de FireSIGHT** joint dans la section Informations connexes.

Dépannez

Pour les informations Verify ou Troubleshoot, référez-vous aux **questions de dépannage avec le Filtrage URL sur l'**article de **système de FireSIGHT** joint dans la section Informations connexes.

Informations connexes

- Dépannez les questions avec le Filtrage URL sur le système de FireSIGHT
- Support et documentation techniques - Cisco Systems