

Tape des fichiers de mise à jour qui pourraient être installés sur un système de FireSIGHT

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Types de mises à jour](#)

[Page de mise à jour sur l'interface web](#)

[Mise à jour produit](#)

[Mise à jour de règle](#)

[Mise à jour de GeoDB](#)

[Mise à jour de renseignements de sécurité](#)

[Mise à jour de Filtrage URL](#)

Introduction

Ce document fournit un aperçu des divers types de mise à jour classe un système de FireSIGHT installé afin de maintenir un système à jour. Quelques fichiers mettent à jour le logiciel et le système d'exploitation de votre système de FireSIGHT, alors que quelques fichiers améliorent la Sécurité.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Appliances de gamme 7000 de puissance de feu de Sourcefire, appliances de gamme 8000, et appliances virtuelles NGIPS
- Version de logiciel 5.0 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.

Types de mises à jour

Sur des systèmes de FireSIGHT, ces types de mises à jour peuvent être installés :

	Description	Exemple
Mise à jour	<ul style="list-style-type: none"> • Introduit de nouveaux caractéristiques et composant 	<code>Sourcefire_3D_Defense_Center_S3_Upgrade-5.4.0-763.sh</code>
Correctif	<ul style="list-style-type: none"> • Inclut des correctifs de bogue. • Résout des problèmes connus. • Inclut les résolutions fournies dans les correctifs précédents 	<code>Sourcefire_3D_Defense_Center_S3_Patch-5.4.1-59.sh</code>
Mise à jour de règle de Sourcefire (SRU)	<ul style="list-style-type: none"> • Peut être installée sur la version de logiciel 5.0 ou plus tard. • Les mises à jour reniflent des règles et des règles partagées d'objet. 	<code>Sourcefire_Rule_Update-2015-05-20-001-vrt.sh</code>
Base de données de vulnérabilité (VDB)	<ul style="list-style-type: none"> • Met à jour les empreintes digital, les 	<code>Sourcefire_VDB_Fingerprint_Database-4.5.0-241.sh</code>

détecteurs,
et les
information
s de
vulnérabilit
é pour des
application
s et des
systèmes
d'exploitati
on.

**Mise à jour de
base de
données de
SourceFire
GeoLocation
(GeoDB)**

- Met à jour
des
données
géographiq
ues
associées
avec les
adresses
IP
routable.

`Sourcefire_Geodb_Update-2015-05-09-001.sh`

**Flux de
renseignements
de sécurité**

- Met à jour
la liste
d'adresse
IP utilisée
pour
mettre des
adresses
IP sur la
liste noire.

Des flux sont téléchargés périodiquement et automatiquement du nuage par le centre de Gestion de FireSIGHT.

**Données de
Filtrage URL**

- Met à jour
les
données
utilisées
pour le
Filtrage
URL dans
des règles
de contrôle
d'accès.

Des flux sont téléchargés périodiquement et automatiquement du nuage par le centre de Gestion de FireSIGHT.

Page de mise à jour sur l'interface web

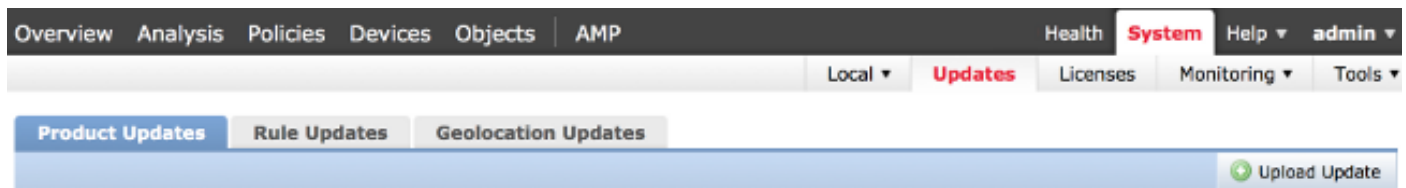
Afin de mettre à jour un centre de Gestion de FireSIGHT, vous pourriez devoir naviguer vers de diverses pages de l'interface web. Il dépend du type de mise à jour que vous voulez télécharger. Cette section fournit la navigation à de diverses pages de mise à jour.

Mise à jour produit

Afin de télécharger ou installer ces composants, choisir le **système** > **les mises à jour**, et choisir l'onglet de **mises à jour produit** :

- Mise à jour
- Correctif
- VDB

Si vous voulez télécharger une mise à jour, corrigez, ou le fichier VDB du site du support technique de Cisco directement, cliquer sur Download des **mises à jour**. Le bouton est disponible au bas de page. Alternativement, si vous téléchargez manuellement un fichier du [site du support technique de Cisco](#) et vous voulez le télécharger au système de FireSIGHT, cliquez sur Upload la **mise à jour**.



Mise à jour de règle

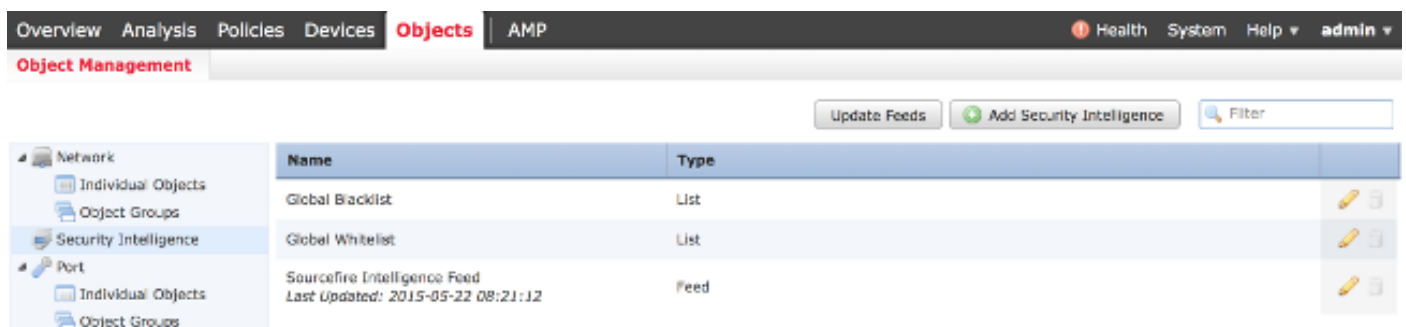
Afin de mettre à jour le SRU, choisir le **système** > **les mises à jour**, et choisir l'onglet de **mises à jour de règle**.

Mise à jour de GeoDB

Afin de mettre à jour le GeoDB, choisir le **système** > **les mises à jour** et choisir l'onglet de **mises à jour de Geolocation**.

Mise à jour de renseignements de sécurité

Afin de mettre à jour le flux de renseignements de sécurité, choisissez les **objets** > **la Gestion d'objet**. Choisissez l'option de **renseignements de sécurité** du panneau gauche, et cliquez sur les **flux de mise à jour**. Si vous voulez mettre à jour votre flux fait sur commande ou vous voulez créer une liste faite sur commande, cliquez sur Add les **renseignements de sécurité**.



Mise à jour de Filtrage URL

Afin de mettre à jour la base de données de Filtrage URL, choisissez le **système** > **les gens du pays** > **la configuration**. Choisissez les **services en nuage** et cliquez sur la **mise à jour maintenant**.

The screenshot shows the configuration page for URL Filtering in the Palo Alto Networks management console. The interface includes a top navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, and AMP. On the right, there are links for Health, System, Help, and admin. Below the navigation bar, there are tabs for Local > Configuration, Updates, Licenses, Monitoring, and Tools. A left-hand sidebar lists various configuration categories, with 'Cloud Services' highlighted in red. The main content area is titled 'URL Filtering' and contains the following settings:

- Enable URL Filtering:
- Enable Automatic Updates:
- Query Cloud for Unknown URLs:
- Last URL Filtering Update: 2015-05-22 01:25:00 [Update Now]

Below the URL Filtering section is the 'Advanced Malware Protection' section with the following settings:

- Share URI Information of malware events with Sourcefire:
- Use legacy port 32137 for network AMP lookups:

A 'Save' button is located at the bottom of the configuration panel.