

Teclea de los archivos de la actualización que se pudieron instalar en un sistema de FireSIGHT

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Tipos de actualizaciones](#)

[Página de la actualización en la interfaz Web](#)

[Actualización del producto](#)

[Actualización de la regla](#)

[Actualización de GeoDB](#)

[Actualización de la inteligencia de Seguridad](#)

[Actualización del Filtrado de URL](#)

Introducción

Este documento proporciona una descripción de los diversos tipos de actualización clasifica un sistema de FireSIGHT instala para mantener un sistema actualizado. Algunos archivos ponen al día el software y el sistema operativo de su sistema de FireSIGHT, mientras que algunos archivos aumentan la Seguridad.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Dispositivos de las 7000 Series de la potencia de fuego de Sourcefire, dispositivos de las 8000 Series, y dispositivos virtuales NGIPS
- Versión de software 5.0 de Sourcefire o más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Tipos de actualizaciones

En los sistemas de FireSIGHT, estos tipos de actualizaciones pueden ser instalados:

	Descripción	Ejemplo:
Actualizar	<ul style="list-style-type: none">• Introduce las nuevas funciones y los componentes.	<code>Sourcefire_3D_Defense_Center_S3_Upgrade-5.4.0-763.sh</code>
Corrección	<ul style="list-style-type: none">• Incluye los arreglos del bug.• Resuelve los problemas conocidos.• Incluye las resoluciones proporcionadas en los hotfixes anteriores.	<code>Sourcefire_3D_Defense_Center_S3_Patch-5.4.1-59.sh</code>
Actualización de la regla de Sourcefire (SRU)	<ul style="list-style-type: none">• Se puede instalar en la versión de software 5.0 o más adelante.• Reglas del Snort de las actualizaciones y reglas compartidas del objeto.	<code>Sourcefire_Rule_Update-2015-05-20-001-vrt.sh</code>
Base de datos de la	<ul style="list-style-type: none">• Pone al	<code>Sourcefire_VDB_Fingerprint_Database-4.5.0-241.sh</code>

vulnerabilidad (VDB)	<p>día las huellas dactilares, los detectores, y la información de la vulnerabilidad para las aplicaciones y los sistemas operativos.</p>	
Actualización de base de datos de SourceFire GeoLocation (GeoDB)	<ul style="list-style-type: none"> • Pone al día los datos geográficos asociados a los IP Address ruteables. 	<pre>Sourcefire_Geodb_Update-2015-05-09-001.sh</pre>
Alimentación de la inteligencia de Seguridad	<p>dirección IP usada para poner los IP Addresses</p>	<p>Las alimentaciones son descargadas periódicamente y automáticamente de la nube por el centro de administración de FireSIGHT.</p>
Datos del Filtrado de URL	<ul style="list-style-type: none"> • Pone al día los datos usados para el Filtrado de URL en las reglas del control de acceso. 	<p>Las alimentaciones son descargadas periódicamente y automáticamente de la nube por el centro de administración de FireSIGHT.</p>

Página de la actualización en la interfaz Web

Para poner al día un centro de administración de FireSIGHT, usted puede ser que tenga que

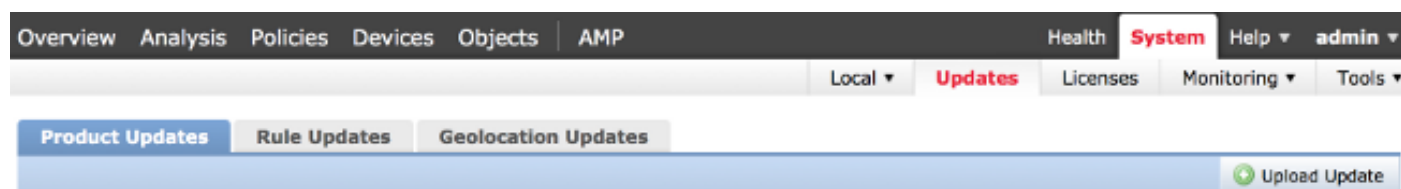
navegar a las diversas páginas de la interfaz Web. Depende del tipo de actualización que usted quiere descargar. Esta sección proporciona la navegación a las diversas páginas de la actualización.

Actualización del producto

Para cargar o instalar estos componentes, elegir el **sistema > las actualizaciones**, y elegir la lengüeta de las **actualizaciones del producto**:

- Actualizar
- Corrección
- VDB

Si usted quiere descargar una actualización, parchee, o archivo VDB del sitio de soporte de Cisco directamente, las **actualizaciones de la descarga del teclado**. El botón está disponible en la parte inferior de la página. Alternativamente, si usted descargó manualmente un archivo del [sitio de soporte de Cisco](#) y usted quiere cargarlo al sistema de FireSIGHT, **actualización de la carga del teclado**.



Actualización de la regla

Para poner al día el SRU, elegir el **sistema > las actualizaciones**, y elegir la lengüeta de las **actualizaciones de la regla**.

Actualización de GeoDB

Para poner al día el GeoDB, elegir el **sistema > las actualizaciones** y elegir la lengüeta de las **actualizaciones de Geolocation**.

Actualización de la inteligencia de Seguridad

Para poner al día la alimentación de la inteligencia de Seguridad, elija los **objetos > la Administración del objeto**. Elija la opción de la **inteligencia de Seguridad del panel izquierdo**, y las **alimentaciones de la actualización del teclado**. Si usted quiere poner al día su alimentación de encargo o usted quiere crear una lista de encargo, el teclado **agrega la inteligencia de Seguridad**.

Overview Analysis Policies Devices **Objects** AMP Health System Help admin

Object Management Update Feeds Add Security Intelligence Filter

	Name	Type	
Network			
Individual Objects			
Object Groups			
Security Intelligence			
Port			
Individual Objects			
Object Groups			
	Global Blacklist	List	
	Global Whitelist	List	
	Sourcefire Intelligence Feed Last Updated: 2015-05-22 08:21:12	Feed	

Actualización del Filtrado de URL

Para poner al día la base de datos del Filtrado de URL, elija el **sistema > el Local > la configuración**. Elija los **servicios de la nube** y ahora haga clic la **actualización**.

Overview Analysis Policies Devices Objects AMP Health **System** Help admin

Local > Configuration Updates Licenses Monitoring Tools

Information

- HTTPS Certificate
- Database
- Management Interfaces
- Process
- Time
- Remote Storage Device
- Change Reconciliation
- Console Configuration
- Cloud Services**

URL Filtering

- Enable URL Filtering
- Enable Automatic Updates
- Query Cloud for Unknown URLs
- Last URL Filtering Update: 2015-05-22 04:55:00 Update Now

Advanced Malware Protection

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

Save