Tipi di file di aggiornamento che possono essere installati su un sistema FireSIGHT

Sommario

Introduzione

Questo documento fornisce una panoramica dei vari tipi di file di aggiornamento installati da un sistema FireSIGHT per mantenere aggiornato il sistema. Alcuni file aggiornano il software e il sistema operativo del sistema FireSIGHT, mentre altri migliorano la sicurezza.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- Appliance Sourcefire FirePOWER serie 7000, appliance serie 8000 e NGIPS Virtual Appliance
- Software Sourcefire versione 5.0 o successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Tipi di aggiornamenti

Sui sistemi FireSIGHT è possibile installare i seguenti tipi di aggiornamenti:

	Descrizione	Esempio
Aggiornamento	• Introduce nuove funzionalità e componenti. • Include le correzioni dei bug. • Risolve i problemi noti.	`Sourcefire_3D_Defense_Center_S3_`**`Upgrade`**`-5.4.0-763.sh`
Patch	• Include le risoluzioni fornite negli aggiornamenti rapidi precedenti. • Può essere installato sul software versione 5.0 o successive.	`Sourcefire_3D_Defense_Center_S3_`**`Patch`**`-5.4.1-59.sh`
Sourcefire Rule Update (SRU)	• Aggiorna le regole di tipo Snort e le regole dell'oggetto condiviso.	`Sourcefire_Rule_Update-2015-05-20-001-vrt.sh`
VDB (Vulnerability Database)	• Aggiorna le impronte digitali, i rilevatori e le informazioni sulle vulnerabilità per le applicazioni e i sistemi	`Sourcefire_`**`VDB`**`_Fingerprint_Database-4.5.0-241.sh`

Aggiornamento database GeoLocation SourceFire (GeoDB)	operativi. • Aggiorna i dati geografici associati agli indirizzi IP instradabili.	`Sourcefire_Geodb_Update-2015-05-09-001.sh`
Feed Security Intelligence	• Aggiorna l'elenco degli indirizzi IP utilizzati per la creazione della blacklist degli indirizzi IP.	I feed vengono scaricati periodicamente e automaticamente dal cloud dal centro di gestione FireSIGHT.
Dati del filtro URL	• Aggiorna i dati utilizzati per il filtro URL nelle regole di controllo di accesso.	I feed vengono scaricati periodicamente e automaticamente dal cloud dal centro di gestione FireSIGHT.

Aggiorna pagina sull'interfaccia Web

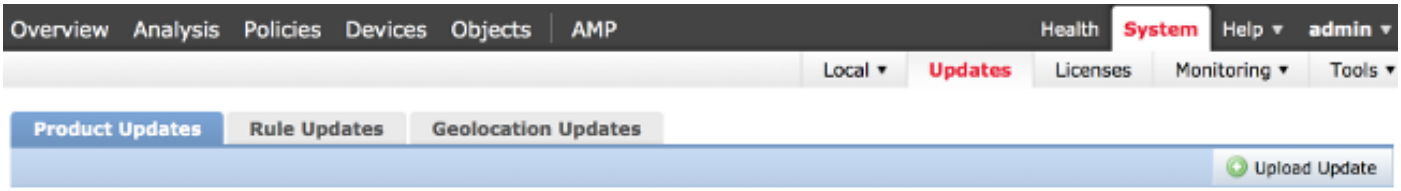
Per aggiornare un centro di gestione FireSIGHT, potrebbe essere necessario passare a diverse pagine dell'interfaccia Web. Dipende dal tipo di aggiornamento che si desidera scaricare. Questa sezione consente di passare a diverse pagine di aggiornamento.

Aggiornamento prodotti

Per caricare o installare questi componenti, scegliere **Sistema > Aggiornamenti**, quindi selezionare la scheda **Aggiornamenti prodotto**:

- Aggiornamento
- Patch
- VDB

Se si desidera scaricare un aggiornamento, una patch o un file VDB direttamente dal sito del supporto Cisco, fare clic su **Download Updates**. Il pulsante è disponibile nella parte inferiore della pagina. In alternativa, se si è scaricato manualmente un file dal sito del supporto Cisco e si desidera caricarlo nel sistema FireSIGHT, fare clic su **Upload Update** (Carica aggiornamento).



Aggiornamento regola

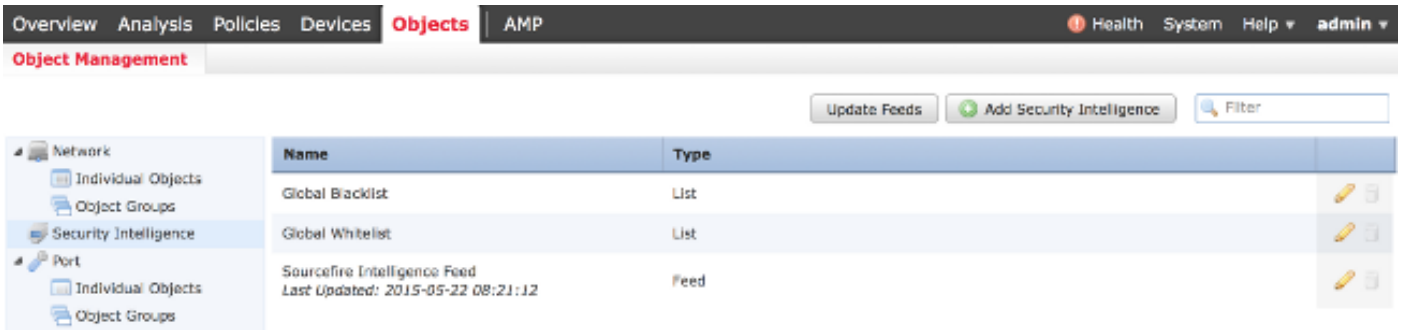
Per aggiornare la SRU, scegliere **Sistema > Aggiornamenti**, quindi scegliere la scheda **Aggiornamenti regole**.

Aggiornamento GeoDB

Per aggiornare GeoDB, scegliere **Sistema > Aggiornamenti**, quindi scegliere la scheda **Aggiornamenti geolocalizzazione**.

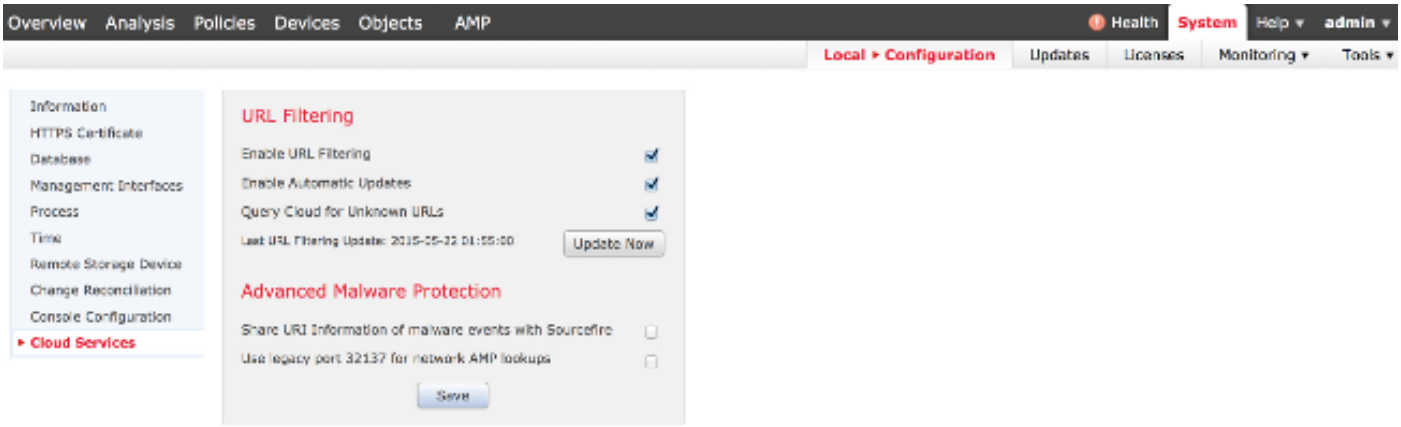
Aggiornamento Security Intelligence

Per aggiornare il feed di Security Intelligence, scegliere **Oggetti > Gestione oggetti**. Scegliere l'opzione **Security Intelligence** nel riquadro sinistro e fare clic su **Aggiorna feed**. Se si desidera aggiornare il feed personalizzato o creare un elenco personalizzato, fare clic su **Aggiungi intelligence di sicurezza**.



Aggiornamento del filtro URL

Per aggiornare il database del filtro URL, scegliere **Sistema > Locale > Configurazione**. Scegliere **Servizi cloud** e fare clic su **Aggiorna ora**.


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: 2015-05-13 01:55:00
Update Now
Advanced Malware Protection
Share URI Information of malware events with Sourcefire
Use legacy port 32137 for network AMP lookups
Save