Types of Update Files That Might Be Installed on a FireSIGHT System

Document ID: 118490

Contributed by Nazmul Rajib, Cisco TAC Engineer.
Jun 03, 2015

Contents

Introduction

This document provides an overview of the various types of update files a FireSIGHT System installs in order to keep a system up−to−date. Some files update the software and operating system of your FireSIGHT System, while some files enhance security.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these hardware and software versions:

- Sourcefire FirePOWER 7000 Series Appliances, 8000 Series Appliances, and NGIPS Virtual Appliances
- Sourcefire Software Version 5.0 or later

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.

Types of Updates

On FireSIGHT Systems, these types of updates can be installed:

	Description	Example
Upgrade	• Introduces new features and components. • Includes bug fixes.	Sourcefire_3D_Defense_Center_S3_***Upgrade***−5.4.0−763.sh
Patch	• Resolves known issues. • Includes the resolutions provided in the previous hotfixes.	Sourcefire_3D_Defense_Center_S3_***Patch***−5.4.1−59.sh
Sourcefire Rule Update (SRU)	• Can be installed on software version 5.0 or later. • Updates Snort rules and shared object rules.	***S***ourcefire_***R***ule_***U***pdate−2015−05−20−001−vrt.sh
Vulnerability Database (VDB)	• Updates the fingerprints, detectors, and vulnerability information for applications and operating systems.	Sourcefire_***VDB***_Fingerprint_Database−4.5.0−241.sh
SourceFire GeoLocation Database Update (GeoDB)	• Updates geographical data associated with routable IP addresses.	Sourcefire_***Geodb***_Update−2015−05−09−001.sh
Security Intelligence Feed	• Updates the list of IP address used for blacklisting IP addresses.	Feeds are downloaded periodically and automatically from the cloud by the FireSIGHT Management Center.
URL Filtering Data	• Updates the data used for URL filtering in Access Control rules.	Feeds are downloaded periodically and automatically from the cloud by the FireSIGHT Management Center.

Update Page on the Web Interface

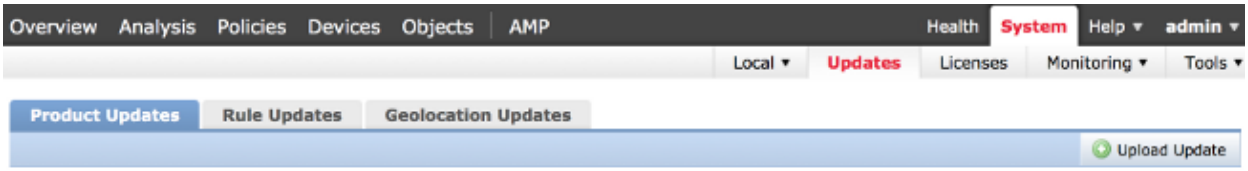
In order to update a FireSIGHT Management Center, you might have to navigate to various pages of the web interface. It depends on the type of update you want to download. This section provides the navigation to various update pages.

Product Update

In order to upload or install these components, choose ***System > Updates***, and choose the ***Product Updates*** tab:

- Upgrade
- Patch
- VDB

If you want to download an upgrade, patch, or VDB file from the Cisco Support site directly, click ***Download Updates***. The button is available at the bottom of the page. Alternatively, if you manually downloaded a file from the Cisco Support site and you want to upload it to the FireSIGHT System, click ***Upload Update***.



Rule Update

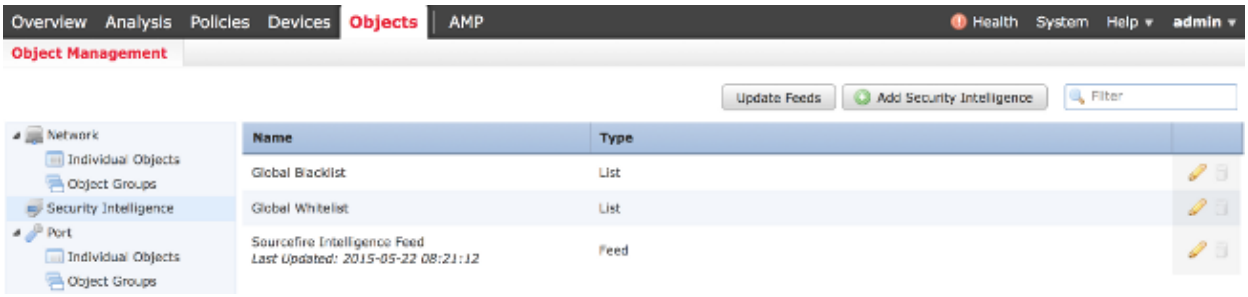
In order to update the SRU, choose ***System*** > ***Updates***, and choose the ***Rule Updates*** tab.

GeoDB Update

In order to update the GeoDB, choose ***System*** > ***Updates*** and choose the ***Geolocation Updates*** tab.

Security Intelligence Update

In order to update the Security Intelligence Feed, choose ***Objects*** > ***Object Management***. Choose the ***Security Intelligence*** option from the left panel, and click ***Update Feeds***. If you want to update your custom feed or you want to create a custom list, click ***Add Security Intelligence***.



URL Filtering Update

In order to update the URL Filtering database, choose ***System*** > ***Local*** > ***Configuration***. Choose ***Cloud Services*** and click ***Update Now***.