Guidelines for Downloading Data from the Firepower Management Center to Managed Devices

Contents

Introduction

Maintaining a Firepower deployment requires that you periodically download data from the Firepower Management Center to the devices it manages. This document provides information you can use to successfully transfer updates from the Firepower Management Center to managed devices.

General Download Guidelines

To support day-to-day operation of your Firepower system, Cisco recommends maintaining a dedicated network bandwidth of at least 256 kbps between the external interface and each managed device. Be sure the bandwidth allotted between the Firepower Management Center and the switch it uses to communicate with its managed devices is sufficient to support at least 256 kbps for each device. Additional bandwidth may be required when downloading software updates from the Firepower Management Center to a managed device, or when simultaneously downloading multiple policy or data updates to a managed device.

> **Caution**: Downloading updates to managed devices may affect traffic inspection, traffic flow, and link state. In the case of software updates, the Data Correlator is disabled while an update is in progress. Therefore Cisco recommends you download updates in a maintenance window or at a time when the load on the managed device being updated is minimal and an interruption will have the least impact on your deployment.

The time required to perform any type of data download from the Firepower Management Center to a managed device depends on the size of the data package and the dedicated network bandwidth between the two appliances. Data downloads to managed devices will fail if they cannot complete within the designated timeout periods Firepower enforces on download activities.

> **Note**: The bandwidth requirements cited in this document presume lossless links between appliances; if your network experiences high latency or high rates of packet loss, additional bandwidth will be required to complete downloads within the timeouts Firepower requires.

If after adjusting your network environment using the information in this document you cannot download an update package to a managed device within the timeout period, contact Cisco TAC.

Downloading Software Updates

Software update package sizes vary widely; see the *Firepower System Release Notes* for your version for the full update process as well as the data package size. Firepower applies a timeout of 1 hour to software downloads. The following table provides formulae to approximate the amount of time a software download will take depending on the package size and the available dedicated bandwidth between devices.

Package Size	**Time to Download at 256 kbps**	**Time to Download at 512 kbps**	**Time to Download at 2 mbps**	**Time to Downloa 3 mbps**
X MB	32X seconds	16X seconds	4X seconds	3X seconds

> **Caution**: Because the update process may affect traffic inspection, traffic flow, and link state, and because the Data Correlator is disabled while an update is in progress, Cisco recommends you perform the software update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Downloading Vulnerability Database Updates

Vulnerability database updates range in size from 30 to 70 MB. Downloading a VDB update from the Firepower Management Center to a managed device fails if it does not complete within 1 hour. Given dedicated network bandwidth, doubling the bandwidth available for the download approximately halves the amount of time required to complete the download. For example, the table below presents the bandwidths and times-to-download for a VDB package of 65 MB:

Package Size	**Time to Download at 256 kbps**	**Time to Download at 512 kbps**	**Time to Download at 2 mbps**	**Time to Downloa 4 mbps**
65 MB	2130 seconds	1065 seconds	273 seconds	136 seconds

VDB update downloads occur asynchronously.

> **Caution**: Installing a VDB update restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See the *Firepower Management Center Configuration Guide* for more information.

Downloading Access Control Policy and Intrusion Rule Updates

The size of an access control policy and intrusion rule update varies depending on a number of

factors, including the number of rules in the update, the conditions within the rules, the number of reusable objects the rules reference, and the number of intrusion policy-variable set combinations the rules reference. While no fixed formula can predict package size for access control policy and intrusion rule updates, the following table provides examples you can use to estimate your own package size. For each sample package, the table provides the minimum dedicated network bandwidth required between the two appliances to complete the download within the 5 minute timeout the system enforces.

Policy Description	Estimated Package Size	Minimum Bandwidth
4 intrusion policies and 1K policy (All 4 default intrusion and 1000 access control rules)	7.8 MB	223 kbps
4 intrusion policies and 5K policy (All 4 default intrusion + 5000 access control rules)	8.2 MB	256 kbps
4 intrusion policies and 10K policy (All 4 default intrusion and 10000 access control rules)	9 MB	256 kbps

The table depicts only a few example policy update scenarios. Policy update packages that include additional policies such as file or system policies will be larger and require additional bandwidth to download within the timeout the Firepower system enforces.

> **Caution**: Deploying access control and intrusion rule updates may increase resource demands and result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See the *Firepower Management Center Configuration Guide* for more information.

Downloading URL Lists

Due to memory limitations, some device models perform most URL filtering with a smaller, less granular, set of categories and reputations. Consequently URL list downloads vary in size depending on the device model; approximate sizes are shown in the following table:

Package Size	Full URL List Download	URL List Update
Higher-memory devices	450 MB	40 – 80 MB
Lower-memory devices	20 MB	20 MB

Lower-memory devices include the 7100 Family and the following ASA models: ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, and ASA5525-X. (For NGIPSv, see the *Firepower System Virtual Installation Guide* for information on allocating the correct amount of memory to perform category and reputation-based URL filtering.)

Downloading a URL list or URL list update ranging in size from 1 to 100 MB fails if it does not complete within 10 minutes (600 seconds). Downloading a URL list or URL list update ranging in size from 100 MB to 4 GB fails if it does not complete within 1 hour (3600 seconds).

Given dedicated network bandwidth, doubling the bandwidth available for the download approximately halves the amount of time required to complete the download, as shown in the

examples below:

Package Size	Time to Download at 256 kbps	Time to Download at 512 kbps	Time to Download at 2 mbps	Time to Downloa 4 mbps
20 MB	640 seconds	320 seconds	80 seconds	42 seconds
450 MB	14745 seconds	7373 seconds	1887 seconds	944 seconds

Downloads of URL list updates occur asynchronously.