Introduction to the Cisco ASA FirePOWER Module

The Cisco ASA FirePOWER module® is a module that can be deployed on Cisco ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60. The module is designed to help you handle network traffic in a way that complies with your organization's security policy—your guidelines for protecting your network. A security policy may also include an acceptable use policy (AUP), which provides employees with guidelines of how they may use your organization's systems.

This guide provides information about onbox configuration of the features and functionality of the ASA FirePOWER module, accessible via ASDM. The explanatory text, diagrams, and procedures in each chapter provide detailed information to help you navigate the user interface, maximize the performance of your system, and troubleshoot complications.

Note If you enable command authorization on the ASA that hosts the ASA FirePOWER module, you must log in with a user name that has privilege level 15 to see the ASA FirePOWER home, configuration, and monitoring pages. Read-only or monitor-only access to ASA FirePOWER pages other than the status page is not supported.

The topics that follow introduce you to the ASA FirePOWER module, describe its key components, and help you understand how to use this guide:

Introduction to the ASA FirePOWER Module

The ASA FirePOWER module runs on an ASA device installed on network segments monitor traffic for analysis.

Deployed inline, the system can affect the flow of traffic using *access control*, which allows you to specify, in a granular fashion, how to handle the traffic entering, exiting, and traversing your network. The data that you collect about your network traffic and all the information you glean from it can be used to filter and control that traffic based on:

- simple, easily-determined transport and network layer characteristics: source and destination, port, protocol, and so on
- the latest contextual information on the traffic, including characteristics such as reputation, risk, business relevance, application used, or URL visited
- Microsoft Active Directory LDAP users in your organization

Each type of traffic inspection and control occurs where it makes the most sense for maximum flexibility and performance. For example, reputation-based blacklisting, because it uses simple source and destination data, can block prohibited traffic early in the process, while detecting and blocking intrusions and exploits is a last-line defense.

ASA FirePOWER Module Components

The topics that follow describe some of the key capabilities of the ASA FirePOWER module that contribute to your organization's security, acceptable use policy, and traffic management strategy:

- Access Control, page 1-2
- Intrusion Detection and Prevention, page 1-2
- Advanced Malware Protection and File Control, page 1-3
- Application Programming Interfaces, page 1-3

Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network. An *access control policy* determines how the system handles traffic on your network.

The simplest access control policy handles all traffic using its *default action*. You can set this default action to block or trust all traffic without further inspection, or to inspect traffic for intrusions.

A more complex access control policy can blacklist traffic based on Security Intelligence data, as well as use *access control rules* to exert granular control over network traffic logging and handling. These rules can be simple or complex, matching and inspecting traffic using multiple criteria; you can control traffic by security zone, network or geographical location, port, application, requested URL, ISE attribute, and user. Advanced access control options include decryption, preprocessing, and performance.

Each access control rule also has an *action*, which determines whether you monitor, trust, block, or allow matching traffic. When you allow traffic, you can specify that the system first inspect it with intrusion or file policies to block any exploits, malware, or prohibited files before they reach your assets or exit your network.

Intrusion Detection and Prevention

Intrusion detection and prevention is the system's last line of defense before traffic is allowed to its destination. *Intrusion policies* are defined sets of intrusion detection and prevention configurations invoked by your access control policy. Using *intrusion rules* and other settings, these policies inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic.

If the system-provided policies do not fully address the security needs of your organization, custom policies can improve the performance of the system in your environment and can provide a focused view of the malicious traffic and policy violations occurring on your network. By creating and tuning custom policies you can configure, at a very granular level, how the system processes and inspects the traffic on your network for intrusions.

Advanced Malware Protection and File Control

To help you identify and mitigate the effects of malware, the ASA FirePOWER module's file control and advanced malware protection components can detect, track, capture, analyze, and optionally block the transmission of files (including malware files and nested files inside archive files) in network traffic.

File Control

File control allows devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. You configure file control as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Network-Based Advanced Malware Protection (AMP)

Network-based *advanced malware protection* (AMP) allows the system to inspect network traffic for malware in several types of files.

Regardless of whether you store a detected file, you can submit it to the Collective Security Intelligence Cloud for a simple known-disposition lookup using the file's SHA-256 hash value. Using this contextual information, you can configure the system to block or allow specific files.

You configure malware protection as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Application Programming Interfaces

There are several ways to interact with the system using application programming interfaces (APIs). For detailed information, you can download additional documentation from either of the following Support Sites:

- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

License Conventions

The License statement at the beginning of a section indicates the license required to use the feature described in the section, as follows:

Protection

A Protection license allows devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering.

Control

A Control license allows devices to perform user and application control. A Control license requires a Protection license.

URL Filtering

A URL Filtering license allows devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts. A URL Filtering license requires a Protection license.

Malware

A Malware license allows devices to perform network-based advanced malware protection (AMP), that is, to detect, capture, and block malware in files transmitted over your network. A Malware license requires a Protection license.

Because licensed capabilities are often additive, this documentation only provides the highest required license for each feature. For example, if a feature requires Protection and Control licenses, only Control is listed. However, if functionality requires licenses that are not additive, the documentation lists them with a plus (+) character.

An "or" statement in a License statement indicates that a particular license is required to use the feature described in the section, but an additional license can add functionality. For example, within a file policy, some file rule actions require a Protection license while others require a Malware license. So, the License statement for the documentation on file rules lists "Protection or Malware."

IP Address Conventions

You can use IPv4 Classless Inter-Domain Routing (CIDR) notation and the similar IPv6 prefix length notation to define address blocks in many places in the ASA FirePOWER module.

CIDR notation uses a network IP address combined with a bit mask to define the IP addresses in the specified block of addresses. For example, the following table lists the private IPv4 address spaces in CIDR notation.

Table 1-1 CIDR Notation Syntax Examples

CIDR Block	IP Addresses in CIDR Block	Subnet Mask	Number of IP Addresses
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

Similarly, IPv6 uses a network IP address combined with a prefix length to define the IP addresses in a specified block. For example, 2001:db8::/32 specifies the IPv6 addresses in the 2001:db8:: network with a prefix length of 32 bits, that is, 2001:db8:: through 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff.

When you use CIDR or prefix length notation to specify a block of IP addresses, the ASA FirePOWER module uses **only** the portion of the network IP address specified by the mask or prefix length. For example, if you type 10.1.2.3/8, the ASA FirePOWER module uses 10.0.0.0/8.

In other words, although Cisco recommends the standard method of using a network IP address on the bit boundary when using CIDR or prefix length notation, the ASA FirePOWER module does not require it.