Get Started Using ASA with FirePOWER Services

The Cisco ASA FirePOWER module can be deployed on select Cisco ASA 5500-X series appliances. For detailed information, see the *Cisco Firepower Compatibility Guide*. The module is designed to help you handle network traffic in a way that complies with your organization's security policy.

This guide provides information about configuration of the features and functionality of the ASA FirePOWER module, accessible using the Adaptive Security Device Manager (ASDM).

Alternatively, to manage an ASA with FirePOWER Services device using the Firepower Management Center, see the *Cisco Firepower Management Center Configuration Guide*.

Quick Start: Basic Setup

To get started setting up your ASA with FirePOWER Services device, see the Cisco ASA FirePOWER Module Quick Start Guide. The Quick Start Guide walks you through the entire setup process, including:

1. Deploy ASA with FirePOWER Services.

Note Skip the section on registering ASA with FirePOWER Services with Firepower Management Center to manage ASA with FirePOWER Services using ASDM.

Caution You can manage any particular appliance using either the Firepower Management Center or using ADSM but not both. *Switching management methods erases the existing appliance configuration*.

2. Start ASDM.
3. Configure ASA with FirePOWER Services.

Set Up Policy and Basic Configuration

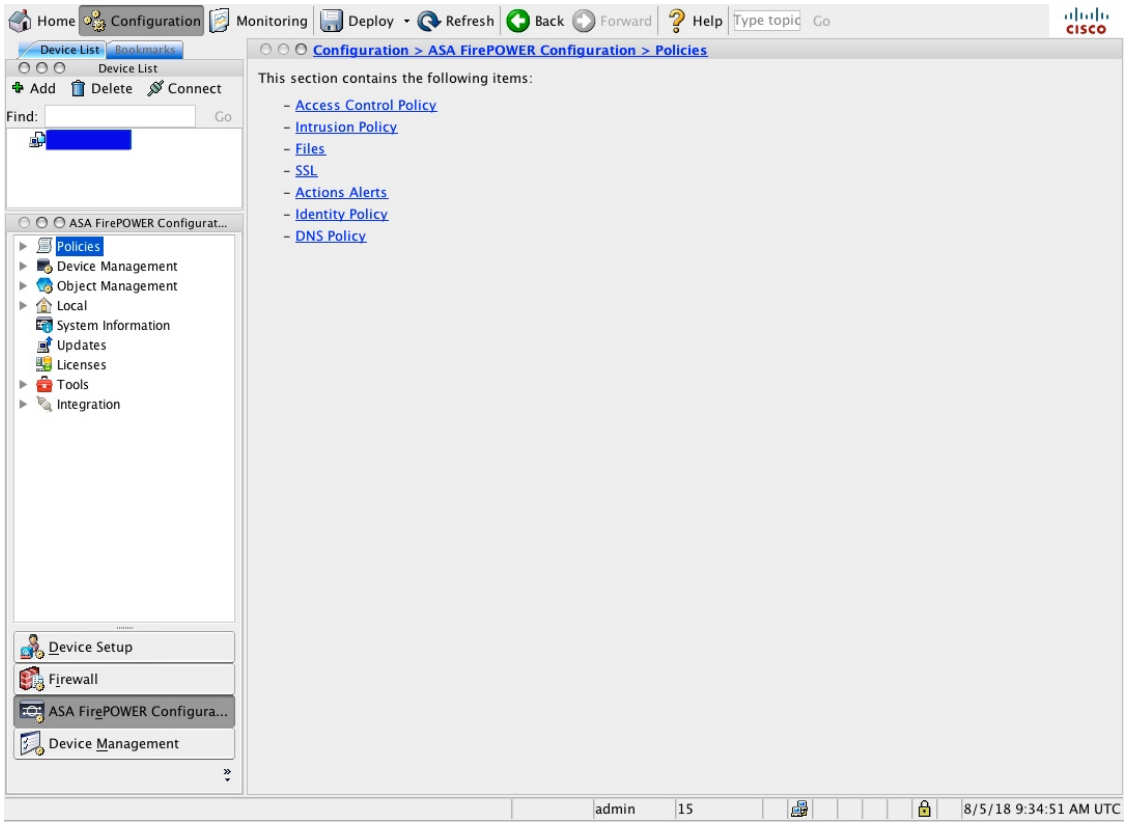
Before you begin

Initially configure the ASA with FirePOWER Services module as discussed in Quick Start: Basic Setup, on page 1.

Step 1 Start ASDM and log in to the ASA with FirePOWER Services module as discussed in its Quick Start Guide.

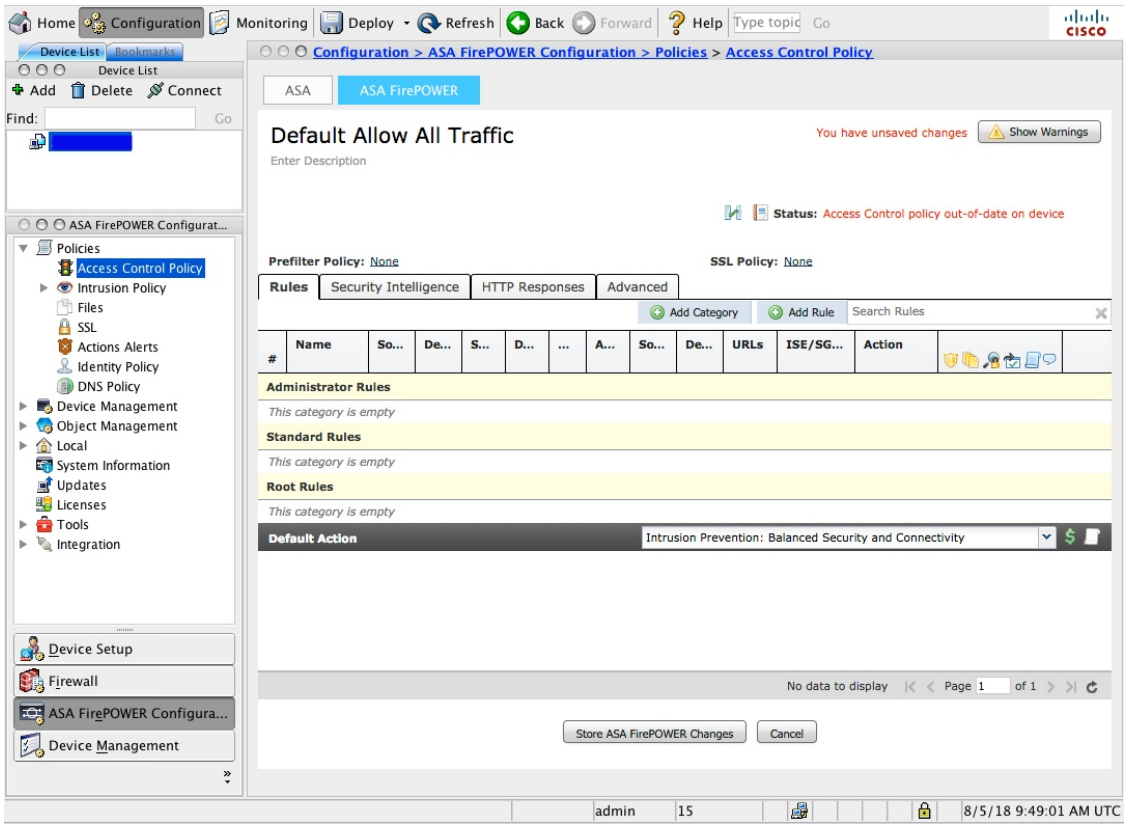
Step 2 In the top navigation bar, click **Configuration**.

Step 3 On the side navigation bar, click **ASA FirePOWER Configuration**.
The **configuration** page is displayed as follows.



Step 4 Create the access control policy as discussed in Creating a Basic Access Control Policy.

a) Expand **Policies**.
b) Click **Access Control Policy**.
c) Click **ASA with FirePOWER**.
The **policy** page is displayed as follows.



d) In most cases, for **Default Action**, we recommend choosing **Intrusion Prevention: Balanced Security and Connectivity**.

Step 5 Customize other common settings:

a) Manage device interfaces
b) Configure a system policy
c) Configure local settings
d) To use Advanced Malware Protection, enable cloud communications
e) Stream logs to a syslog server or SNMP data using external alerts
f) Schedule backups
g) Schedule automatic software downloads
h) Schedule automatic software installations
i) Schedule automatic rule updates
j) Schedule automatic URL filtering updates
k) Schedule automatic geolocation database updates

What to do next

Configure ASA options as discussed in the Cisco Adaptive Security Device Manager Configuration Guides.

ASA With FirePOWER Services Devices

ASA with FirePOWER Services devices are also referred to as *Next Generation Intrusion Prevention (NGIPS)* devices. These devices run NGIPS software on an ASA device.

The ASA device provides the first-line system policy, then passes traffic to an ASA FirePOWER module for discovery and access control.

ASA FirePOWER has a user interface and a command line interface (CLI) unique to the ASA platform. You use these ASA-specific tools to install the system and to perform other platform-specific administrative tasks.

ASA FirePOWER does not support the following Firepower features:

- Features for Firepower hardware: Use the ASA CLI and ASDM to configure device high availability, stacking, switching, routing, VPN, NAT, and so on. See the ASA documentation for more information.
- Interface configuration: You *cannot* use the Firepower Management Center web interface to configure ASA FirePOWER interfaces. The Firepower Management Center does not display ASA interfaces when the ASA FirePOWER is deployed in SPAN port mode.
- Process management: You *cannot* use the Firepower Management Center to shut down, restart, or otherwise manage ASA FirePOWER processes.

ASA With FirePOWER Services Features

This section lists some commonly used ASA With FirePOWER Services features.

Appliance and System Management Features

To locate unfamiliar documents, see the documentation roadmap.

If you want to...	Configure...	As discussed in...
Back up data on your appliance	Backup and restore	Using Backup and Restore
Upgrade to a new software version	Software updates	Updating ASA FirePOWER Module Software
Baseline your appliance	Restore to factory defaults (reimage)	• Cisco ASA and Firepower Threat Defense Reimage Guide • Section on reimaging the FirePOWER module in the Cisco Adaptive Security Device Manager Configuration Guides
Ensure continuity of appliance operations	High availability	Cisco Adaptive Security Device Manager Configuration Guides

If you want to...	Configure...	As discussed in...
Update the VDB, intrusion rule updates, or GeoDB on your appliance	Vulnerability Database (VDB) updates, intrusion rule updates, or Geolocation Database (GeoDB) updates	Understanding Update Types
Apply licenses in order to take advantage of license-controlled functionality	Licensing	Understanding Licensing
Configure a device to route traffic between two or more interfaces	Routing	ASDM Configuration Guides
Translate private addresses into public addresses for internet connections	Network Address Translation (NAT)	Cisco Adaptive Security Device Manager Configuration Guides

Features for Detecting, Preventing, and Processing Potential Threats

To locate unfamiliar documents, see the documentation roadmap.

If you want to...	Configure...	As discussed in...
Inspect, log, and take action on network traffic	Access control policy, the parent of several other policies	Getting Started with Access Control Policies
Blacklist connections to or from IP addresses, URLs, and/or domain names	Security Intelligence in your access control policy	Choosing a Security Intelligence Strategy
Monitor malicious traffic and intrusions on your network	Intrusion policy	About Intrusion Policies
Block encrypted traffic without inspection Inspect encrypted or decrypted traffic	SSL policy	Understanding Traffic Decryption
Allow or block files on your network	File policy	Controlling Traffic Using Intrusion and File Policies
Configure passive or active user authentication to perform user awareness and user control	User awareness, user identity, identity policies	Introduction to Identity Data

Integration with External Tools

To locate unfamiliar documents, see the documentation roadmap.

If you want to...	Configure...	As discussed in...
Stream event data to a custom-developed client application	eStreamer integration	Understanding Advanced Device Settings

Firepower Online Help, How To, and Documentation

You can reach the online help from the web interface:

- By clicking the context-sensitive help link on each page
- By choosing **Help** > **Online**

You can find additional documentation related to the Firepower system using the documentation roadmap: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

Related Documentation

The documents listed in this section might be helpful when configuring your ASA with FirePOWER Services appliance.

Hardware Guides and Data Sheets

The following guides provide more information about ASA with FirePOWER Services hardware.

- https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/sfr/firepower-qsg.html

For More Details

Some topics are not included in this guide because they are covered in more detail in the Firepower Management Center Configuration Guide. The following table lists these topics; for additional information not covered in this guide, see also Related Documentation, on page 6

For more information about...	See the FMC Configuration Guide *part* > *chapter*
Access control rules	**Access Control** > **Access Control Rules**
Intrusion policies	**Intrusion Detection and Prevention** > **Getting Started with Intrusion Policies**
Troubleshooting tools	**System Monitoring and Troubleshooting** > **Troubleshooting the System**
Realms for user control	**Discovery and Identity** > **Create and Manage Realms**

For more information about...	See the FMC Configuration Guide *part* > *chapter*
Identity policies	**Discovery and Identity** > **Create and Manage Identity Policies**
Internal Certificate Authorities (CAs)	**Deployment Management** > **Reusable Objects**
Trusted CAs	**Deployment Management** > **Reusable Objects**
Geolocation database updates	**Deployment Management** > **Reusable Objects**

Supported Devices Statements in the Documentation

The Supported Devices statement at the beginning of a chapter or topic indicates that a feature is supported only on the specified device series, family, or model. For example, stacking is supported only on 8000 Series devices.

For more information on platforms supported by this release, see the release notes.

Access Statements in the Documentation

The Access statement at the beginning of each procedure in this documentation indicates the predefined user roles required to perform the procedure. Any of the listed roles can perform the procedure.

Users with custom roles may have permission sets that differ from those of the predefined roles. When a predefined role is used to indicate access requirements for a procedure, a custom role with similar permissions also has access. Some users with custom roles may use slightly different menu paths to reach configuration pages. For example, users who have a custom role with only intrusion policy privileges access the network analysis policy via the intrusion policy instead of the standard path through the access control policy.

Firepower System 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 Firepower System.

When you use CIDR or prefix length notation to specify a block of IP addresses, the Firepower System 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 Firepower System 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 Firepower System does not require it.

Additional Resources

The Firewalls Community is an exhaustive repository of reference material that complements our extensive documentation. This includes links to 3D models of our hardware, hardware configuration selector, product collateral, configuration examples, troubleshooting tech notes, training videos, lab and Cisco Live sessions, social media channels, Cisco Blogs and all the documentation published by the Technical Publications team.

Some of the individuals posting to community sites or video sharing sites, including the moderators, work for Cisco Systems. Opinions expressed on those sites and in any corresponding comments are the personal opinions of the original authors, not of Cisco. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Cisco or any other party.

Note Some of the videos, technical notes, and reference material in the Firewalls Community points to older versions of the Firepower Management Center. Your version of the Firepower Management Center and the version referenced in the videos or technical notes might have differences in the user interface that cause the procedures not to be identical.