Getting Started With Firepower

Cisco Firepower is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. The system 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.

In a typical deployment, multiple traffic-sensing *managed devices* installed on network segments monitor traffic for analysis and report to a *manager*:

- Firepower Management Center
- Adaptive Security Device Manager (ASDM)

Managers provide a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks.

This guide focuses on the *Firepower Management Center* managing appliance. For information about ASA with FirePOWER Services managed via ASDM, see the guide for that management method.

- *ASA with FirePOWER Services Local Management Configuration Guide*

Introduction to Managed Devices

Managed devices installed on network segments monitor traffic for analysis. Deployed passively, managed devices gather detailed information about your organization's assets: hosts, operating systems, applications, users, sent files (including malware), vulnerabilities, and so on. The Firepower System correlates this information for your analysis so you can monitor the websites your users visit and the applications they use, assess traffic patterns, and receive notifications of intrusions and other attacks.

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 and LDAP users in your organization; you can grant different levels of access to different users
- Characteristics of encrypted traffic; you can also decrypt this traffic for further analysis
- Whether unencrypted or decrypted traffic contains a prohibited file, detected malware, or intrusion event

Note For the system to affect traffic, you must deploy relevant configurations to managed devices using routed, switched, or transparent interfaces, or inline interface pairs.

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. In contrast, detecting and blocking intrusions and exploits is a last-line defense.

Network management features on 7000 and 8000 Series devices allow them to serve in switched and routed environments, perform network address translation (NAT), and to build secure virtual private network (VPN) tunnels between virtual routers you configure. You can also configure bypass interfaces, aggregated interfaces, 8000 Series fastpath rules, and strict TCP enforcement.

7000 and 8000 Series Managed Devices

Cisco Firepower 7000 and 8000 Series appliances are physical devices purpose-built for the Firepower System. 7000 and 8000 Series devices have a range of throughputs, but share most of the same capabilities. In general, 8000 Series devices are more powerful than 7000 Series; they also support additional features such as 8000 Series fastpath rules, link aggregation, and stacking.

NGIPSv

You can deploy NGIPSv (a 64-bit virtual device as an ESXi host) using the VMware vSphere Hypervisor or vCloud Director environment. You can also enable VMware Tools on all supported ESXi versions.

By default, NGIPSv uses e1000 (1 Gbit/s) interfaces. You can also use the VMware vSphere Client to replace the default sensing and management interfaces with vmxnet3 (10 Gbit/s) interfaces.

Regardless of license, NGIPSv does not support any of the system's hardware-based features: redundancy and resource sharing, switching, routing, and so on.

Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services (or an *ASA FirePOWER module*) functions similarly to NGIPSv. In an ASA FirePOWER deployment, the ASA device provides the first-line system policy and passes traffic to the Firepower System for discovery and access control.

Regardless of the licenses installed and applied, ASA FirePOWER does not support any of the following Firepower System features:

- ASA FirePOWER does not support the Firepower System 7000 and 8000 Series hardware-based features: device high availability, stacking, switching, routing, VPN, NAT, and so on. However, the ASA platform does provide these features, which you can configure using the ASA CLI and ASDM. See the ASA documentation for more information.
- 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.
- You cannot use the Firepower Management Center to shut down, restart, or otherwise manage ASA FirePOWER processes.

ASA FirePOWER has a software 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.

Note If you edit an ASA FirePOWER and switch from multiple context mode to single context mode (or vice versa), the device renames all of its interfaces. You **must** reconfigure all Firepower System security zones, correlation rules, and related configurations to use the updated ASA FirePOWER interface names.

Firepower Threat Defense

The Firepower Threat Defense appliance provides a unified next-generation firewall and next-generation IPS device. In addition to the IPS features available on Firepower Software models, firewall and platform features include Site-to-Site VPN, robust routing, NAT, clustering (for the Firepower 9300), and other optimizations in application inspection and access control.

The Firepower Threat Defense software is supported on the following platforms:

- Firepower 9300
- Firepower 4100 series
- ASA 5512-X through 5555-X
- ASA 5508-X and 5516-X
- ASA 5506-X series

Firepower Threat Defense Virtual

The Firepower Threat Defense Virtual (a 64-bit virtual appliance) provides unified next-generation firewall and next-generation IPS capabilities to virtualized environments. Firepower Threat Defense Virtual is designed to work in multiple hypervisor environments, reduce administrative overhead, and increase operational efficiency.

You can deploy Firepower Threat Defense Virtual using the VMware vSphere hypervisor and the KVM (Kernel-based Virtual Machine) hypervisor environments. You can also deploy Firepower Threat Defense Virtual through Amazon Web Services (AWS) cloud platform.

You can use the Firepower Management Center for comprehensive multi-device deployment and management of both the virtual appliance and the physical Firepower Threat Defense appliances.

Introduction to the Firepower Management Center

A Firepower Management Center is a fault-tolerant, purpose-built network appliance that provides a centralized management console and database repository for your Firepower System deployment. You can also deploy 64-bit virtual Firepower Management Centers using the VMware vSphere and the KVM (Kernel-based Virtual Machine) hypervisor environments, and also through Amazon Web Services (AWS) cloud platform. Firepower Management Centers have a range of device management, event storage, host monitoring, and user monitoring capabilities. Any Firepower Management Center can manage any type of Firepower System device.

Firepower Management Centers aggregate and correlate network traffic information and performance data, assessing the impact of events on particular hosts. You can monitor the information that your devices report, and assess and control the overall activity that occurs on your network. Firepower Management Centers also control the network management features on your devices: switching, routing, NAT, VPN, and so on.

Key features of the Firepower Management Center include:

- Device, license, and policy management
- Event and contextual information displayed in tables, graphs, and charts
- Health and performance monitoring
- External notification and alerting
- Correlation, indications of compromise, and remediation features for real-time threat response
- Custom and template-based reporting

Firepower Management Center Capabilities

When running this version, all Firepower Management Centers have similar capabilities, with the primary differences being capacity and speed. Firepower Management Center models vary in terms of how many devices they can manage, how many events they can store, and how many hosts and users they can monitor.

Configuration of features available in the Firepower Management Center web interface may be limited by the license and model of the device you are managing.

The MC4000 introduces Cisco's Unified Computing System (UCS) platform into the Firepower System. The MC4000 does not support Cisco functionality that uses tools on the baseboard management controller (BMC), such as the UCS Manager or the Cisco Integrated Management Controller (CIMC).

Related Topics

About Device Management
Configuring Database Event Limits

Firepower System Components

The topics that follow describe some of the key capabilities of the Firepower System that contribute to your organization’s security, acceptable use policy, and traffic management strategy.

Tip Many Firepower System features are appliance model, license, and user role dependent. This documentation includes information about which Firepower System licenses and devices are required for each feature, and which user roles have permission to complete each procedure.

Redundancy and Resource Sharing

The redundancy and resource-sharing features of the Firepower System allow you to ensure continuity of operations and to combine the processing resources of multiple 7000 and 8000 Series devices.

Device Stacking

Device stacking allows you to increase the amount of traffic inspected on a network segment by connecting two to four devices in a stacked configuration. When you establish a stacked configuration, you combine the resources of each stacked device into a single, shared configuration.

7000 and 8000 Series Device High Availability

7000 and 8000 Series *device high availability* allows you to establish redundancy of networking functionality and configuration data between two or more 7000 or 8000 Series devices or stacks. Configuring two or more peer devices or stacks into a high-availability pair results in a single logical system for policy applies, system updates, and registration. With device high availability, the system can fail over either manually or automatically.

In most cases, you can achieve Layer 3 redundancy without configuring a high-availability pair by using SFRP. SFRP allows devices to act as redundant gateways for specified IP addresses. With network redundancy, you can configure two or more devices or stacks to provide identical network connections, ensuring connectivity for other hosts on the network.

Network Traffic Management for 7000 & 8000 Series Devices

The Firepower System's network traffic management features allow 7000 and 8000 Series devices to act as part of your organization's network infrastructure. You can configure 7000 and 8000 Series devices to serve in a switched, routed, or hybrid (switched and routed) environment; to perform network address translation (NAT); and to build secure virtual private network (VPN) tunnels.

Switching

You can configure the Firepower System in a Layer 2 deployment so that it provides packet switching between two or more network segments. In a Layer 2 deployment, you configure switched interfaces and virtual switches on 7000 and 8000 Series devices to operate as standalone broadcast domains. A virtual switch uses the MAC address from a host to determine where to send packets. You can also group multiple physical interfaces into a single logical link that provides packet switching between two endpoints in your network. The endpoints can be two 7000 and 8000 Series devices, or a managed device connected to a third-party access switch.

Routing

You can configure the Firepower System in a Layer 3 deployment so that it routes traffic between two or more interfaces. In a Layer 3 deployment, you configure routed interfaces and virtual routers on 7000 and

8000 Series devices to receive and forward traffic. The system routes packets by making packet forwarding decisions according to the destination IP address. Routers obtain the destination from the outgoing interface based on the forwarding criteria, and access control rules designate the security policies to apply.

When you configure virtual routers, you can define static routes. In addition, you can configure Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) dynamic routing protocols. You can also configure a combination of static routes and RIP or static routes and OSPF. You can set up DHCP relay for each virtual router you configure.

If you use both virtual switches and virtual routers in your deployment, you can configure associated hybrid interfaces to bridge traffic between them. These utilities analyze traffic to determine its type and the appropriate response (route, switch, or otherwise). You can also group multiple physical interfaces into a single logical link that routes traffic between two endpoints in your network. The endpoints can be two 7000 and 8000 Series devices, or a managed device connected to a third-party router.

NAT

In a Layer 3 deployment, you can configure network address translation (NAT) using 7000 and 8000 Series devices. You can expose an internal server to an external network, or allow an internal host or server to connect to an external application. You can also configure NAT to hide private network addresses from an external network by using a block of IP addresses, or by using a limited block of IP addresses and port translation.

VPN

A virtual private network (VPN) is a network connection that establishes a secure tunnel between endpoints via a public source, like the Internet or other network. You can configure the Firepower System to build secure VPN tunnels between the virtual routers of 7000 and 8000 Series devices.

Multitenancy

The *domains* feature allows you to implement multitenancy within a Firepower System deployment, by segmenting user access to managed devices, configurations, and events.

In addition to any restrictions imposed by your user role, your current domain level can also limit your ability to modify configurations. The system limits most management tasks, like system software updates, to the Global domain.

Discovery and Identity

Cisco's discovery and identity technology collects information about hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities, in order to provide you with a complete view of your network:

- *Network discovery* policies monitor traffic on your network and collect host, application, and non-authoritative user data.
- *Identity* policies associate users on your network with a *realm* and an authentication method in order to collect authoritative user data.

You configure *realms* alongside your identity policies in order to establish connections to LDAP or AD servers and to perform user data downloads.

You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible.

You can also use the Firepower Management Center's web interface to view and analyze the data collected by the system.

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 directs its target devices to handle 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 and discovery data.

A more complex access control policy can blacklist traffic based on IP, URL, and DNS 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, VLAN, port, application, requested URL, 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.

SSL Inspection

SSL inspection is a policy-based feature that allows you to handle encrypted traffic without decryption, or decrypt encrypted traffic for further access control inspection. You can choose to block a source of untrusted encrypted traffic without decrypting or further analyzing the traffic, or you can choose to not decrypt encrypted traffic and inspect it with access control instead.

For further insight into encrypted traffic, you can use public key certificates and paired private keys you upload to the system to decrypt encrypted traffic traversing your network, then inspect the decrypted traffic with access control as if it was never encrypted. If the system does not block the decrypted traffic post-analysis, it reencrypts the traffic before passing it to the destination host. The system can log details about encrypted connections as it acts on them.

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.

Cisco delivers several intrusion policies with the Firepower System. By using system-provided policies you can take advantage of the experience of the Cisco Talos Intelligence Group (Talos). For these policies, Talos sets intrusion and preprocessor rule states (enabled or disabled), as well as provides the initial configurations for other advanced settings. An enabled rule causes the system to generate intrusion events for (and optionally block) traffic matching the rule.

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.

Cisco Advanced Malware Protection and File Control

To help you identify and mitigate the effects of malware, the Firepower System's file control, network file trajectory, and Advanced Malware Protection (AMP) 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 managed 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.

AMP for Firepower

AMP for Firepower is a network-based AMP solution, which allows the system to inspect network traffic for malware in several types of files. Appliances can store detected files for further analysis, either to their hard drive or (for some models) a malware storage pack.

You can analyze files locally on your device using *local malware analysis* to preclassify malware. Regardless of whether you store a detected file, you can submit it to the AMP cloud for a simple known-disposition lookup using the file's SHA-256 hash value. You can also submit files to the Cisco Threat Grid cloud for *dynamic analysis*, which produces a threat score. Using this contextual information, you can configure the system to block or allow specific files.

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

AMP for Endpoints Integration

AMP for Endpoints is an enterprise-class endpoint-based AMP solution. Individual users install lightweight connectors on their computers and mobile devices that communicate with the AMP cloud. The Firepower Management Center can then import records of scans, malware detections, and quarantines, as well as indications of compromise (IOC), and can display trajectories for detected threats.

Use the AMP for Endpoints management console to configure your AMP for Endpoints deployment. The console helps you quickly identify and quarantine malware. You can identify outbreaks when they occur, track their trajectories, understand their effects, and learn how to successfully recover. You can also use AMP for Endpoints to create custom protections, block execution of certain applications based on group policy, and create custom whitelists.

Network File Trajectory

The network file trajectory feature allows you to track a file's transmission path across a network. The system uses SHA-256 hash values to track files; so, to track a file, the system must either:

- Calculate the file's SHA-256 hash value and query the AMP cloud using that value

- Receive endpoint-based threat and quarantine data about that file, using the Firepower Management Center's integration with your organization's AMP for Endpoints deployment

Each file has an associated trajectory map, which contains a visual display of the file's transfers over time and additional information about the file.

Cisco AMP Private Cloud Virtual Appliance

If your organization's security policy does not allow the system to connect directly to the AMP cloud, whether for AMP for Firepower or AMP for Endpoints, you can configure a Cisco AMP Private Cloud Virtual Appliance (AMPv).

AMPv is a virtual machine that acts as a compressed, on-premises version of, or anonymized proxy to, the AMP cloud. Data and actions that usually involve a direct connection to the AMP cloud (such as events from AMP for Endpoints, file disposition lookups, retrospective events, and so on) are instead handled by a local connection to AMPv. With AMPv, no endpoint event data is shared over an external connection.

Cisco AMP Threat Grid On-Premises Appliance

If your organization has privacy or security concerns with submitting files to the public Cisco Threat Grid cloud, you can deploy an on-premises Cisco Threat Grid appliance. Like the public cloud, the on-premises appliance runs eligible files in a sandbox environment, and returns a threat score and dynamic analysis report to the Firepower System. However, the on-premises appliance does not communicate with the public cloud, or any other system external to your network.

Application Programming Interfaces

There are several ways to interact with the system using application programming interfaces (APIs).

eStreamer

The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Firepower Management Center to a custom-developed client application. After you create a client application, you can connect it to the eStreamer server on the Firepower Management Center, start the eStreamer service, and begin exchanging data.

eStreamer integration requires custom programming, but allows you to request specific data from an appliance. If, for example, you display network host data within one of your network management applications, you could write a program to retrieve host criticality or vulnerability data from the Firepower Management Center and add that information to your display.

External Database Access

The database access feature allows you to query several database tables on a Firepower Management Center, using a third-party client that supports JDBC SSL connections.

You can use an industry-standard reporting tool such as Crystal Reports, Actuate BIRT, or JasperSoft iReport to design and submit queries. Or, you can configure your own custom application to query Cisco data. For example, you could build a servlet to report intrusion and discovery event data periodically or refresh an alert dashboard.

Host Input

The host input feature allows you to augment discovery data by importing data from third-party sources using scripts or command-line import files.

The web interface also provides some host input functionality; you can modify operating system or application protocol identities, validate or invalidate vulnerabilities, and delete various items from network maps, including clients and server ports.

Remediation

The system includes an API that allows you to create *remediations* that your Firepower Management Center can automatically launch when conditions on your network violate an associated correlation policy or compliance white list. Remediations can automatically mitigate attacks when you are not immediately available to address them, and ensure that your system remains compliant with your organization's security policy. In addition to remediations that you create, the Firepower Management Center ships with several predefined remediation modules.

The Context Menu

Certain pages in the Firepower System web interface support a right-click (most common) or left-click context menu that you can use as a shortcut for accessing other features in the Firepower System. The contents of the context menu depend where you access it—not only the page but also the specific data.

For example:

- IP address hotspots provide information about the host associated with that address, including any available whois and host profile information.
- SHA-256 hash value hotspots allow you to add a file's SHA-256 hash value to the clean list or custom detection list, or view the entire hash value for copying.

On pages or locations that do not support the Firepower System context menu, the normal context menu for your browser appears.

Policy Editors

Many policy editors contain hotspots over each rule. You can insert new rules and categories; cut, copy, and paste rules; set the rule state; and edit the rule.

Intrusion Rules Editor

The intrusion rules editor contains hotspots over each intrusion rule. You can edit the rule, set the rule state, configure thresholding and suppression options, and view rule documentation.

Event Viewer

Event pages (the drill-down pages and table views available under the Analysis menu) contain hotspots over each event, IP address, URL, DNS query, and certain files' SHA-256 hash values. While viewing most event types, you can:

- View related information in the Context Explorer.
- Drill down into event information in a new window.
- View the full text in places where an event field contains text too long to fully display in the event view, such as a file's SHA-256 hash value, a vulnerability description, or a URL.

While viewing connection events, you can add items to the default Security Intelligence Block and Do Not Block lists:

- An IP address, from an IP address hotspot.
- A URL or domain name, from a URL hotspot.
- A DNS query, from a DNS query hotspot.

While viewing captured files, file events, and malware events, you can:

- Add a file to or remove a file from the clean list or custom detection list.
- Download a copy of the file.
- View nested files inside an archive file.
- Download the parent archive file for a nested file.
- View the file composition.
- Submit the file for local malware and dynamic analysis.

While viewing intrusion events, you can perform similar tasks to those in the intrusion rules editor or an intrusion policy:

- Edit the triggering rule.
- Set the rule state, including disabling the rule.
- Configure thresholding and suppression options.
- View rule documentation.

Intrusion Event Packet View

Intrusion event packet views contain IP address hotspots. The packet view uses a left-click context menu.

Dashboard

Many dashboard widgets contain hotspots to view related information in the Context Explorer. Dashboard widgets can also contain IP address and SHA-256 hash value hotspots.

Context Explorer

The Context Explorer contains hotspots over its charts, tables, and graphs. If you want to examine data from graphs or lists in more detail than the Context Explorer allows, you can drill down to the table views of the relevant data. You can also view related host, user, application, file, and intrusion rule information.

The Context Explorer uses a left-click context menu, which also contains filtering and other options unique to the Context Explorer.

Related Topics

Security Intelligence Lists and Feeds

Switching Domains on the Firepower Management Center

In a multidomain deployment, user role privileges determine which domains a user can access and which privileges the user has within each of those domains. You can associate a single user account with multiple domains and assign different privileges for that user in each domain. For example, you can assign a user read-only privileges in the Global domain, but Administrator privileges in a descendant domain.

Users associated with multiple domains can switch between domains within the same web interface session.

Under your user name in the toolbar, the system displays a tree of available domains. The tree:

- Displays ancestor domains, but may disable access to them based on the privileges assigned to your user account.
- Hides any other domain your user account cannot access, including sibling and descendant domains.

When you switch to a domain, the system displays:

- Data that is relevant to that domain only.
- Menu options determined by the user role assigned to you for that domain.

Procedure

From the drop-down list under your user name, choose the domain you want to access.

Firepower Online Help 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.

Top-Level Documentation Listing Pages for FMC Deployments

The following documents may be helpful when configuring Firepower Management Center deployments, Version 6.0+.

Note Some of the linked documents are not applicable to Firepower Management Center deployments. For example, some links on Firepower Threat Defense pages are specific to deployments managed by Firepower Device Manager, and some links on hardware pages are unrelated to FMC. To avoid confusion, pay careful attention to document titles. Also, some documents cover multiple products and therefore may appear on multiple product pages.

Firepower Management Center

- Firepower Management Center hardware appliances:

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Firepower Management Center Virtual appliances:
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

Firepower Threat Defense, also called NGFW (Next Generation Firewall) devices

- Firepower Threat Defense software:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Firepower Threat Defense Virtual:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- Firepower 4100 series:

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Firepower 9300:

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

Classic devices, also called NGIPS (Next Generation Intrusion Prevention System) devices

- ASA with FirePOWER Services:
  - ASA 5500-X with FirePOWER Services:
    - 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

- Firepower 8000 series:

https://www.cisco.com/c/en/us/support/security/firepower-8000-series-appliances/tsd-products-support-series-home.html

- Firepower 7000 series:

  https://www.cisco.com/c/en/us/support/security/firepower-7000-series-appliances/tsd-products-support-series-home.html

- AMP for Networks:

  https://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-series-home.html

- NGIPSv (virtual device):

  https://www.cisco.com/c/en/us/support/security/ngips-virtual-appliance/tsd-products-support-series-home.html

License Statements in the Documentation

The License statement at the beginning of a section indicates which Classic or Smart license you must assign to a managed device in the Firepower System to enable the feature described in the section.

Because licensed capabilities are often additive, the license statement provides only the highest required license for each feature.

An "or" statement in a License statement indicates that you must assign a particular license to the managed device to enable the feature described in the section, but an additional license can add functionality. For example, within a file policy, some file rule actions require that you assign a Protection license to the device while others require that you assign a Malware license.

For more information about licenses, see About Firepower Licenses.

Related Topics

About Firepower Licenses

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, many features are supported only on Firepower Threat Defense 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.

For more information about user roles, see Predefined User Roles and Custom User Roles.

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.