Cisco Firepower Management Center

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

• Firepower Device Manager

• Adaptive Security Device Manager (ASDM)

The Firepower feature set is powerful and flexible enough to support basic and advanced configurations. Use the following sections to quickly set up a Firepower Management Center and its managed devices to begin controlling and analyzing traffic.

Firepower Management Center

The Cisco Firepower Management Center Configuration Guide includes detailed information on Firepower configuration using the Firepower Management Center web interface.

Firewall Threat Defense



Managers provide a centralized management console with graphical user interface that you can use to perform:

1. Administrative,
2. Management,
3. Analysis,
4. And reporting tasks.

The Cisco Firepower Management Center (formerly FireSIGHT Management Center) is the administrative nerve center for select Cisco security products running on a number of different platforms. It provides complete and unified management of firewalls, application control, and intrusion prevention, URL filtering, and advanced malware protection.

The Management Center is the centralized point for event and policy management for the following solutions:

1. Cisco Firepower Next-Generation Firewall (NGFW)
2. Cisco ASA with FirePOWER Services
3. Cisco Firepower Next-Generation IPS (NGIPS)
4. Cisco FirePOWER Threat Defense for ISR
5. Cisco Advanced Malware Protection (AMP)

In addition to the NGIPS features available on Firepower software models, NGFW and platform features include Site-to-Site and remote access VPN, robust routing, NAT, clustering, and other optimizations in application inspection and access control.

The Cisco Firepower Management Center provides extensive intelligence about the users, applications, devices, threats, and vulnerabilities that exist in your network. It also uses this information to analyze your network’s vulnerabilities. It then provides tailored recommendations on what security policies to put in place and what security events you should investigate.

The Management Center provides easy-to-use policy screens to control access and guard against known attacks. It integrates with advanced malware protection and sandboxing technology, and it provides tools to track malware infections throughout your network. It unifies all these capabilities in a single management interface. You can go from managing a firewall to controlling applications to investigating and remediating malware outbreaks with ease.

**Figure 1.**     Centralized Policy, Event, and Device Management



Enterprise-Class Management

The Cisco Firepower Management Center discovers real-time information about changing network resources and operations.

You get a full contextual basis for making informed decisions (see Figure 1). In addition to providing a wide breadth of intelligence, the Management Center delivers a fine level of detail, including:

* **Trends and high-level statistics.** This information helps you understand your security posture at a given moment in time as well as how it’s changing, for better or worse
* **Event detail, compliance, and forensics.** These provide an understanding of what happened during a security event. They help improve defenses, support breach containment efforts, and aid in legal enforcement actions
* **Workflow data.** You can easily export this data to other solutions to improve incident response management

Single Policy for Multiple Security Functions



**Exceptional Visibility and Insight**

You can’t protect what you can’t see. The Cisco Firepower Management Center automatically collects, collates, and displays contextual information about everything running in your environment. Table 1 illustrates the breadth of contextual awareness provided into threat vectors that more traditional security technologies do not detect. This critical insight into your network is available for use in your protection policies and gives you a level of protection that other solutions cannot.

Application Identification and Control



Firepower NGIPS, FirePOWER Threat Defense for ISR

NGIPS software running on 7000 and 8000 Series Firepower devices, or hosted on VMware.

Advanced Malware Protection (AMP).

The management center automatically correlates security events with the vulnerabilities in your environment. It prioritizes attacks so your team can easily see which events they need to investigate first. And it recommends the security policies to put in place.

Threat Intelligence Director

Using open industry-standards interfaces, Threat Intelligence Director ingests intelligence from multiple sources. It then facilitates the appropriate monitoring and containment actions. It correlates observations with third-party sources to reduce the total number of alerts you need to review.

Firepower Devices

In a typical deployment, multiple traffic-handling devices installed on network segments monitor traffic for analysis and report to either a physical or virtual Firepower Management Center. The Firepower Management Center provides a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks.

