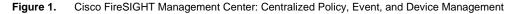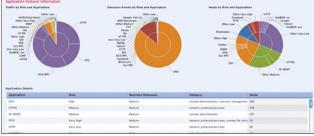# Cisco FireSIGHT Management Center

Product Overview

Cisco® FireSIGHT Management Center provides total visibility into everything on your network: physical and virtual hosts, operating systems, applications, services, protocols, users, geolocation information, content, and network behavior as well as network attacks and malware. This security management console and database repository is the centralized point of event and policy management for your security operations (Figure 1). It allows you to automatically aggregate and correlate information generated by the Cisco ASA with FirePOWER Services and Cisco FirePOWER physical or virtual appliances deployed in your network. Cisco FireSIGHT centrally manages network security and operational functions, including event monitoring, analysis, incident prioritization, and reporting, so that you can better protect your business. It also reduces your costs by streamlining operations and automating many commonly recurring security analysis and management tasks.

Enterprise-Class Management

Figure 1. Cisco FireSIGHT Management Center: Centralized Policy, Event, and Device Management

Cisco FireSIGHT passively discovers real-time information about changing network resources and operations to provide a full contextual basis for making informed decisions. Cisco FireSIGHT Management Center appliances should be selected based on the number of monitored sensor appliances and hosts in the environment and the anticipated security events to be analyzed or stored (see Table 2). All configurations provide the following management capabilities:

- Centralized device, license, event and policy management
- Role-based management (segmented and isolated views and duties based on administrator role or group)
- Customizable dashboard with custom and template-based reports
- Comprehensive reporting and alerts for both general and focused information
- Event and contextual information displayed in hyperlinked tables, graphs, and charts
- Network behavior and performance monitoring
- Robust high availability options to help ensure no single point of failure
- Correlation and remediation features for real-time threat response
- Open APIs for integration with third-party solutions and customer work streams, such as firewalls, network infrastructure, log management, security information and event management (SIEM), trouble ticketing, and patch management

In addition to providing a wide breadth of intelligence, Cisco FireSIGHT delivers a deep level of detail, including:

- **Trends and high-level statistics:** Helps managers and executives understand security posture at a moment in time as well as how it's changing, for better or worse

- **Event detail, compliance, and forensics:** Provides an understanding of what happened during a security event to improve defenses and support breach containment efforts and aid in law enforcement and legal actions

- **Workflows:** Easily exports data to drive responses to an event, improving response management

Unparalleled Visibility and Insight

Table 1 illustrates how Cisco FireSIGHT provides full contextual awareness into threat vectors that more traditional security technologies do not detect.

Table 1.   Cisco FireSIGHT Management Center: Full Stack Visibility

Category	Cisco FireSIGHT	Typical IPS	Typical Next-Generation Firewall
Threats	Yes	Yes	Yes
Users	Yes	Yes	Yes
Web applications	Yes	No	Yes
Application protocols	Yes	No	Yes
File transfers	Yes	No	Yes
Malware	Yes	No	No
Command and control servers	Yes	No	No
Client applications	Yes	No	No
Network servers	Yes	No	No
Operating systems	Yes	No	No

Category	Cisco FireSIGHT	Typical IPS	Typical Next-Generation Firewall
Routers and switches	Yes	No	No
Mobile devices	Yes	No	No
Printers	Yes	No	No
VoIP phones	Yes	No	No
Virtual machines	Yes	No	No

Automate Security for Dynamic Defense

Cisco FireSIGHT continually monitors how the network is changing over time. New threats are automatically assessed to determine which can affect your business. Response efforts are then focused on remediation, and network defenses are adapted to those changing conditions. Critical security activities such as policy tuning are automated, saving time and effort, while protections and countermeasures are maintained in an optimal state.

Choice of Deployment Modes

Cisco FireSIGHT Management Center can be deployed as a physical or virtual appliance. Physical Cisco FireSIGHT appliances maximize the number of sensors and event storage that can be centrally managed. Virtual Cisco FireSIGHT appliances provide the convenience of provisioning on an existing infrastructure. They can be easily deployed using VMware vSphere provisioning and can be deployed within the VMware infrastructure to protect assets in a physical network. Cisco FireSIGHT Version 5.x virtual appliances can be hosted on VMware ESX and ESXi. Cisco FireSIGHT Management Center can manage up to 25 physical or virtual devices.

Product Specifications

Table 2 compares the capacity and throughput for available Cisco FireSIGHT Management Center Appliances, both physical and virtual.

Table 2.   Cisco FireSIGHT Management Center Appliance Models

Feature	FireSIGHT FS750	FireSIGHT FS1500	FireSIGHT FS3500	FireSIGHT FS-VMW-SW
Maximum number of devices managed	10	35	150	25
Maximum number of IPS events	20 million	30 million	150 million	-
Event storage	100 GB	125 GB	400 GB	-
Maximum network map (hosts/users)	2,000/2,000	50,000/50,000	300,000/300,000	-
Maximum flow rate (flows per second)	2,000 fps	6,000 fps	10,000 fps	-
High availability	Lights-out management (LOM)	RAID 1, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	-

Note: A Cisco FireSIGHT Management Center appliance must be present for a sensor to function. All sensor licensing and management is handled by the Cisco FireSIGHT Management Center.

Ordering Information

Table 3 provides ordering information for virtual and physical Cisco FireSIGHT Management Center appliances and additional spare hardware.

Table 3.   Cisco FireSIGHT Management Center Ordering Information

Cisco FireSIGHT Management Center (Hardware) Appliances	
Part Number	**Product Description**
FS750-K9	Cisco FireSIGHT Management Center 750 Chassis, 1U
FS1500-K9	Cisco FireSIGHT Management Center 1500 Chassis, 1U
FS3500-K9	Cisco FireSIGHT Management Center 3500 Chassis, 1U
Cisco FireSIGHT Management Center (Hardware) Spare	
FS-PWR-AC-650W=	Cisco FireSIGHT 650W AC Power Supply
Cisco FireSIGHT Management Center (Software) Virtual Appliance	
FS-VMW-SW-K9	Cisco FireSIGHT Management Center, Virtual (VMWare) FireSIGHT License

To place an order, visit the Cisco ordering homepage.

For more information, please visit the following links:

- Cisco ASA with FirePOWER Services
- Cisco FirePOWER Appliances
- Cisco FireSIGHT Management Center
- Cisco Security Services:
  http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html.

Printed in USA

C78-732251-00   09/14