Cisco Security Manager

Businesses are facing new challenges in security operations. The growing number and increasing complexity of security technologies, combined with the reduction and redirection of IT headcount once dedicated to security management, has dramatically increased the potential for human error, which can lead to security exposures and incidents. To counteract these challenges, it's invaluable for security operations teams to have an integrated, end-to-end management solution that facilitates consistent policy enforcement, helps enable the rapid troubleshooting of security events, and delivers summarized reports across the security solutions deployment.

Cisco® Security Manager is a comprehensive management solution that does all that and more. It provides scalable, centralized management that allows administrators to efficiently manage a wide range of Cisco security devices, gain visibility across the network deployment, and share information with other essential network services, such as compliance systems and advanced security analysis systems, with a high degree of security. Designed for operational efficiency, Cisco Security Manager also includes a powerful suite of automated capabilities, such as health and performance monitoring, software image management, auto-conflict detection, and integration with ticketing systems.

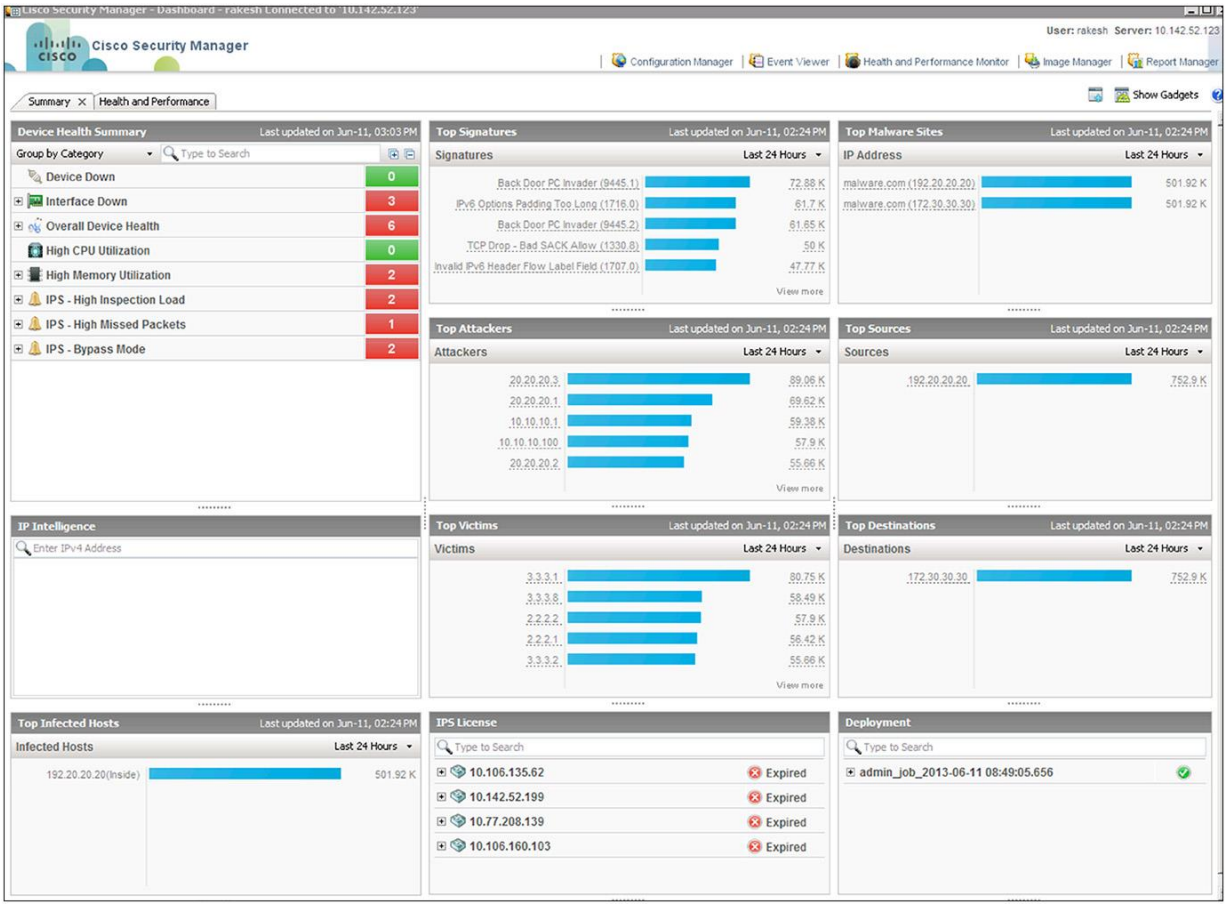
Cisco Security Manager supports a wide range of Cisco security devices, including Cisco ASA 5500 Series and ASA 5500-X Series Adaptive Security Appliances; Cisco IPS 4200, 4300, and 4500 Series Sensors; Cisco SR 500 Series Secure Routers; and the Cisco AnyConnect® Secure Mobility Client.

There are several key features in Cisco Security Manager that make for simplified and efficient security management. The following sections describe these features:

Dashboard

The Cisco Security Manager dashboard (Figure 1) is a widget-based home screen that gives a bird's-eye view of the health, functioning, and other key performance indicators of a network security setup. Several widgets such as the Device Health Summary, Top Attackers, Top Victims, Top Signatures, and others, provide an excellent summary of priority security aspects that an administrator needs to be aware of. These widgets act as a starting point for any security readiness analysis. For example, in the Signatures widget, a user can click the number of times a specific signature has been hit, and Cisco Security Manager will take the user to the Event Viewer, where events corresponding to that signature can be analyzed. Similarly, the administrator can click an IP address on the Top Attackers widget and look at value-added information related to that IP address. So in summary, the dashboard screen is the starting point for security administrators on Cisco Security Manager. Additionally, these dashboards can be personalized to suit each administrator's needs.

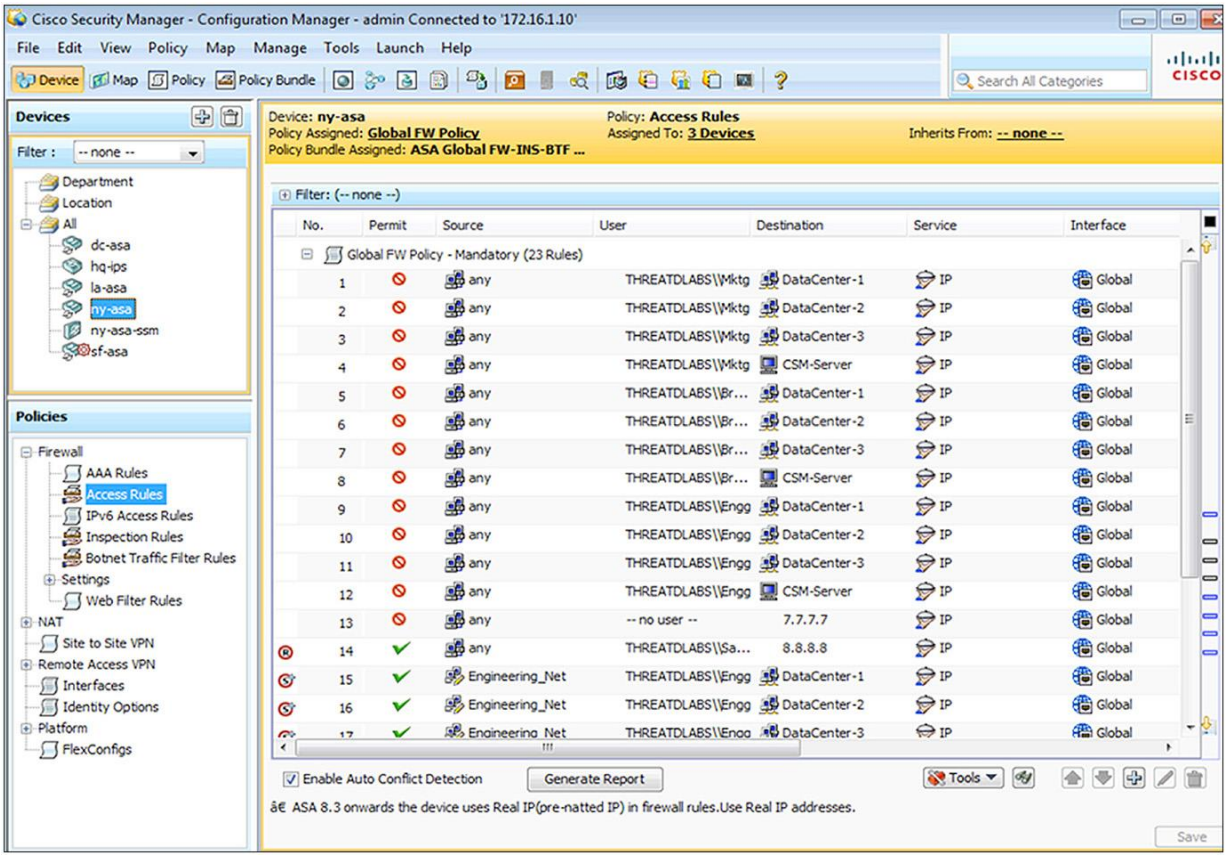
Figure 1. Cisco Security Manager Dashboard



Integrated Policy and Object Management

Cisco Security Manager helps enable the reuse of security rules and objects and enhances the ability to monitor security threats throughout the deployment, minimizing the potential for errors and maximizing efficiency. Administrators can implement security deployments on either an on-demand or scheduled basis and can roll back to a previous configuration if required. Role-based access control and deployment workflows help ensure that compliance processes are followed (see Figure 2).

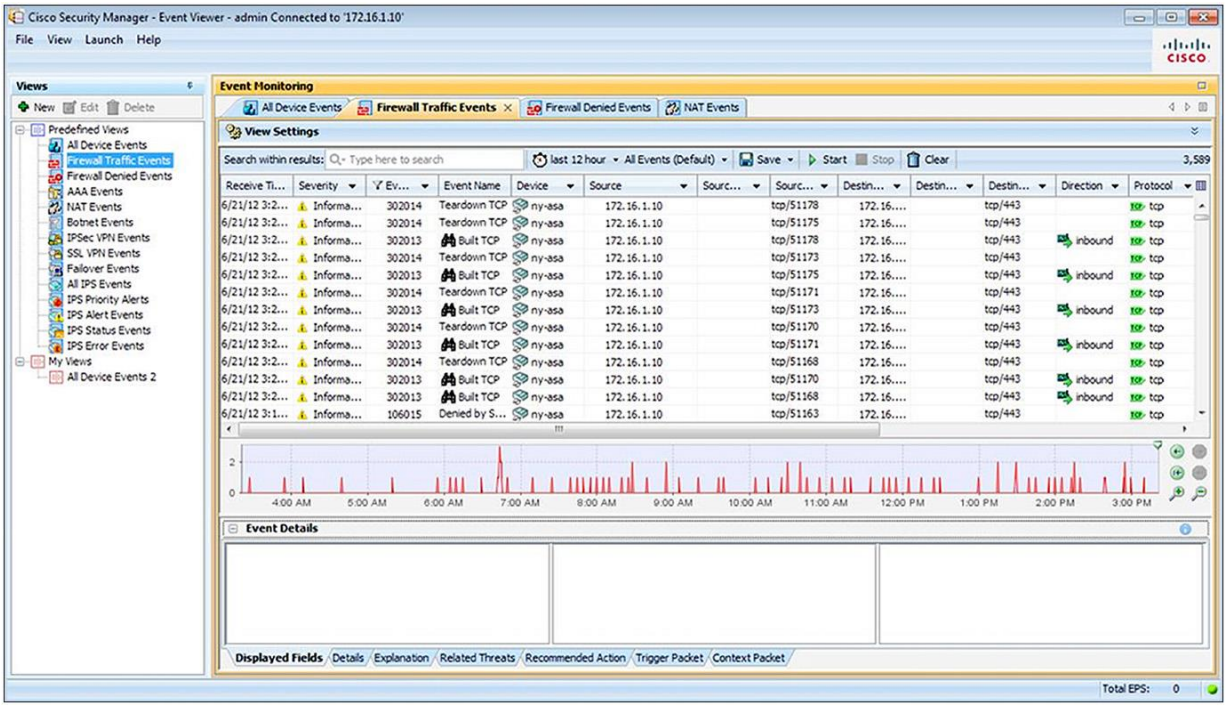
Figure 2. Security Policy Management with Cisco Security Manager



Event Management and Troubleshooting

Integrated event management helps enable the viewing of real-time and historical events for rapid incident analysis and troubleshooting and provides rapid navigation from events to source policies. In addition, administrators can quickly identify and isolate interesting events by using advanced filtering and search capabilities. Cross-linkages between the Event Manager and Configuration Manager reduce troubleshooting time for firewall rules and intrusion prevention system (IPS) signatures (see Figure 3).

Figure 3. Event Management and Troubleshooting with Cisco Security Manager



The Event Manager in Cisco Security Manager provides:

- Support for syslog messages created by Cisco ASA appliances, the Cisco Firewall Services Module (FWSM), and Cisco Catalyst® 6500 Series ASA Services Module, as well as Security Device Event Exchange (SDEE) messages from Cisco IPS sensors
- Real-time and historical event viewing
- Cross-linkages to firewall access rules and IPS signatures for quick navigation to the source policies
- A prebundled set of views for firewall, IPS, and VPN
- Customizable views for monitoring select devices or a select time range
- Intuitive GUI controls for searching, sorting, and filtering events
- Administrative options to turn event collection on or off for select security devices
- Tools such as ping, traceroute, and packet tracer for further troubleshooting capabilities

More information on event management for multivendor environments, event correlation, and historical event analysis is available at: http://www.cisco.com/go/securitypartners.

Reporting

Cisco Security Manager generates detailed system reports based on events and other essential information gathered throughout the security deployment (Figure 4). Table 1 lists the available system reports. In addition, administrators can define and save predefined reports to meet specific reporting needs. Whether system-generated or predefined, all reports can be exported and scheduled for email delivery as PDF or CSV files. Users can also find more detail from a specific chart to view additional information for further analysis.

Figure 4. Report Manager in Cisco Security Manager

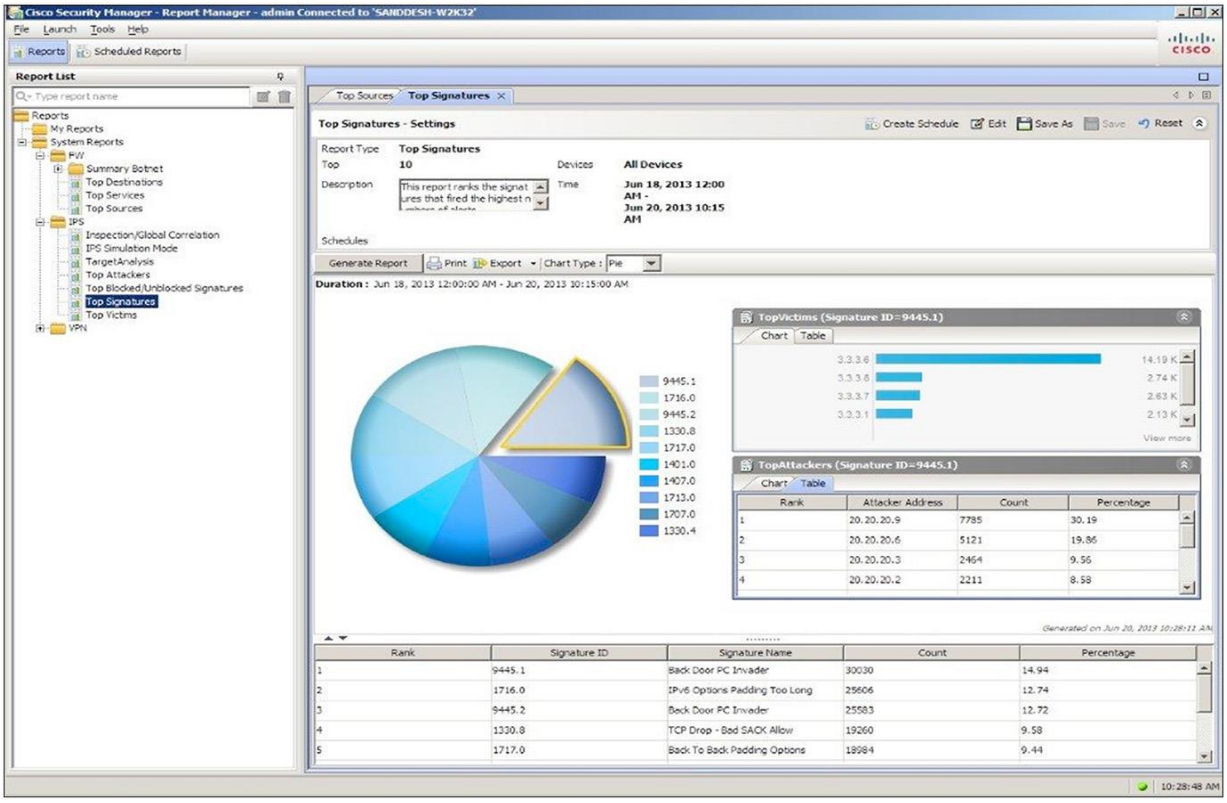


Table 1. Cisco Security Manager System Reports

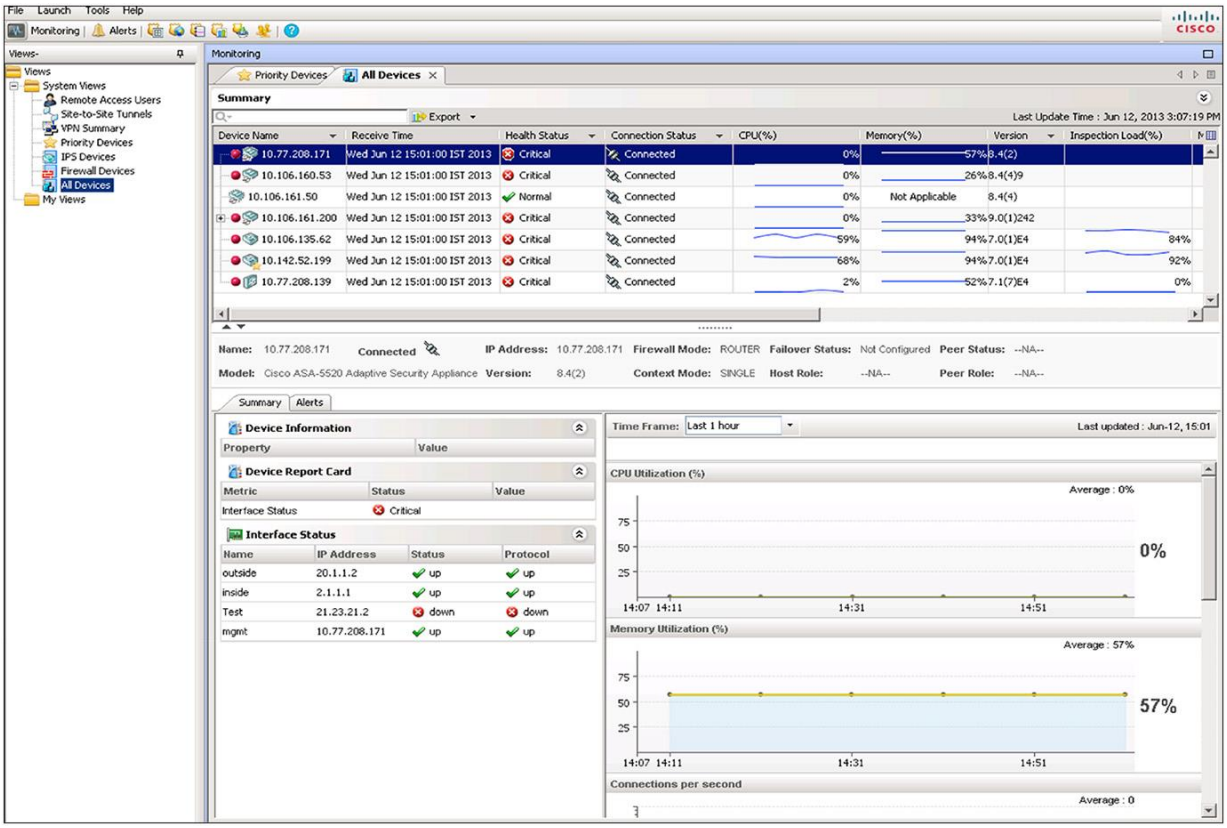
Firewall	IPS	VPN
• Top Infected Hosts • Top Malware Ports • Top Malware Sites • Top Destinations • Top Services • Top Sources	• Inspection/Global Correlation • IPS Simulation Mode • Target Analysis • Top Attackers • Top Blocked/Unblocked Signatures • Top Signatures • Top Victims	• Top Bandwidth Users (SSL/IPsec) • Top Duration Users (SSL/IPsec) • Top Throughput Users (SSL/IPsec) • User Report • VPN Device Usage Report

Health and Performance Monitoring

The integrated Health and Performance Monitor can help administrators increase their productivity by continuously analyzing the security environment and sending alerts when preset thresholds are reached. Customizable alert notifications can be set for such events as critical firewall failover, IPS sensor application failures, or excessive CPU or memory utilization.

Using a simple color-coded interface, administrators can immediately identify any devices that are in critical condition and view commonly monitored attributes (CPU or memory utilization, for example) to rapidly ascertain the general health and performance of all devices across the security deployment. Detailed charts can be used to gain additional insights regarding the health, traffic, and performance metrics of each device, as desired. Figure 5 shows the primary monitoring interface.

Figure 5. Health and Performance Monitor in Cisco Security Manager

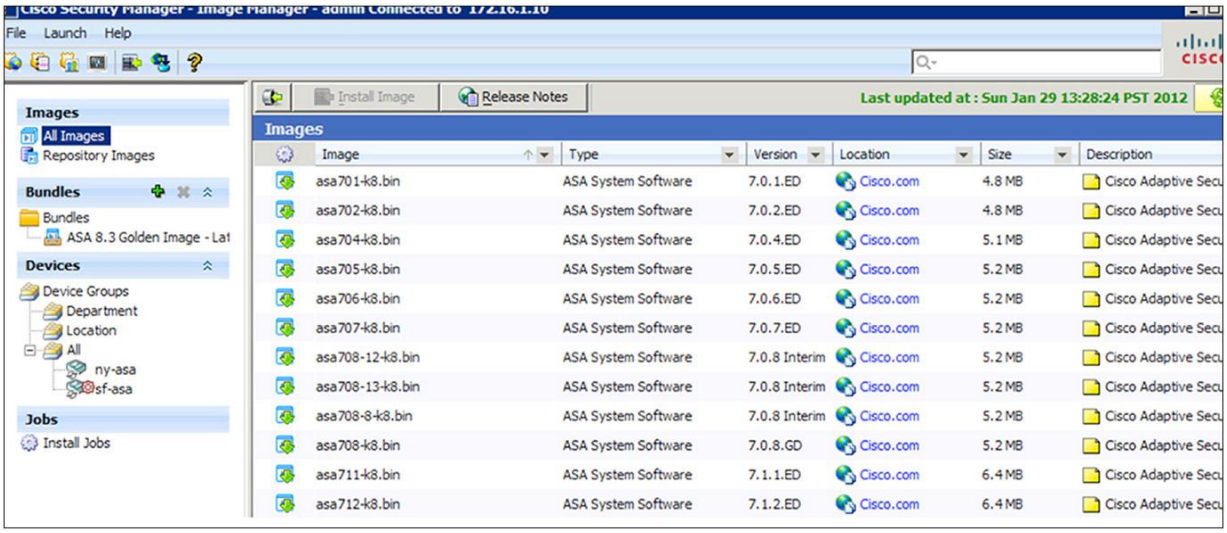


These health and monitoring features are available for the new Cisco ASA clustering features as well.

Software Image Upgrades

Firewall software images can be upgraded using an intuitive wizard. The wizard leads administrators through the steps required to download the images, create the image bundle, and verify that the image is appropriate for each device. The tool then performs the backup, takes the devices down, and performs the update. The updates can be performed on each firewall individually or run in groups to maximize speed and efficiency. The process is automated so it can be run overnight or during noncritical times to reduce disruption to the operating environment. Figure 6 shows the primary image management interface of Cisco Security Manager.

Figure 6. Software Image Upgrade Wizard in Cisco Security Manager



API-Based Access to Cisco Security Manager

With the highly secure API-based access, Cisco Security Manager can share information with other essential network services, such as compliance and advanced security analysis systems, to streamline their security operations and compliance adherence. Using representational state transfer, external firewall compliance systems can directly request access to data from any security device managed by Cisco Security Manager. These third party client programs can also add, delete or modify firewall access policies and policy objects in CSM through the APIs. These APIs seamlessly integrate with CSM's workflow feature, thereby allowing administrators to enforce strict controls when policy configuration is automated through CSM APIs.

Additional Features and Benefits

Table 2 summarizes the additional features and benefits of Cisco Security Manager.

Table 2. Cisco Security Manager: Additional Features and Benefits

Feature	Benefit
Firewall Configuration	
Manages the Cisco security deployment	Facilitates the centralized management of the Cisco security environment, including: • Cisco ASA 5500 Series and 5500-X Series Adaptive Security Appliances • Cisco IPS 4200, 4300, and 4500 Series Sensors • Cisco AnyConnect Secure Mobility Client • Cisco SR 500 Series Secure Routers • Cisco Catalyst 6500 Series Firewall Services Modules and ASA Services Modules • Cisco Integrated Services Router (ISR) platforms running a Cisco IOS® Software security image

Feature	Benefit
Zone-based policies	Sets zone-based firewall policies on supported device platforms if desired.
Botnet Traffic Filter	Supports the Cisco Botnet Traffic Filter on the Cisco ASA platform, for application-layer inspection and blockage of “phone-home” activity by botnets.
Integration with Cisco TrustSec® security group tags	Provides integration with Cisco TrustSec security group tags, so that Cisco Security Manager users can configure detailed and highly relevant policies across deployments.
Cisco ASA clustering	Offers advanced failover capabilities to support multiple Cisco ASA appliances and load-sharing mechanisms to reduce downtime and improve availability.
Content filtering	Supports content filtering on Cisco IOS Software-based device platforms to filter traffic based on deep content inspection. Enables the management of multiple device platforms using a single rule table.
Efficient policy definition	Increases the efficiency with which administrators can define policies by clearly displaying which rules match a specific source, destination, and service flow, including wildcards.
Syslog forwarding	Cisco Security Manager supports forwarding logs generated by ASA firewalls to two remote collectors in addition to the in-built Cisco Security Manager’s Event Viewer.
Simplified setup	Streamlines configuration and simplifies initial security management setup by enabling device information to be imported from a device repository or configuration file, added in the software, or discovered from the device itself.
Streamlined operations	Significantly reduces manual tasks while reducing errors and optimizing the security environment, through: • Rule conflict detection, hit-count analysis, rule combiner, and other powerful tools to analyze and optimize rule sets. • Role-based access control and workflow to help ensure error-free deployments and process compliance.
Interface roles	Can apply rule policies to groups of interfaces and centrally manages them to maximize flexibility and scalability.
IPS Configuration	
Configuration and update policies	Easily and effectively manages IPS-based configuration and update policies for: • Cisco IPS 4200 and 4300 Series Sensors • Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM) • Cisco ASA Advanced Inspection and Prevention Security Services Card (AIP-SSC) • Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM-2) • Cisco IDS Network Module • Cisco IPS Advanced Integration Module (AIM) • Cisco IOS IPS
Signature updates	Can incrementally provision new and updated signatures before deploying them to the enterprise.
Threat research	Allows administrators can configure their environment based on insights gained from Cisco Security Intelligence Operations (SIO), the Cisco Security IntelliShield® Alert Manager Service, and Cisco IPS Security Research Team recommendations before distributing the signature update.
Update wizard	Enables efficient, automatic IPS updates, scheduling, and distribution of policies with status and detail notification.
Reusable policies	Makes IPS signature policies and event action filters inheritable and assignable to any device: all IPS polices can be assigned to and shared with other IPS devices.
Policy rollback	Includes IPS policy rollback, a configuration archive, and cloning or creation of signatures.
Easy operations	Provides an easy means of navigation between signatures and events generated for those signatures; an intuitive user interface provides simple mechanisms for tuning and managing signatures.
Risk-rating categories	Dynamically calculates risk-rating values that can be grouped into a risk range and defined as a category. Signatures can be assigned a risk-rating category and accordingly assigned with actions that are to be taken if the signature is hit.
Global event actions	Can add multiple event actions to a risk-rating category that will apply globally to all signatures in that risk rating range. Also, specific actions can be filtered from a signature for an event if necessary.
Signature annotations	Can add notes to a signature by multiple users, which can later be viewed in a consolidated manner for that signature.
CSV export	Makes comma-separated value (CSV) export available for select IPS features such as signatures, event action filters, and signature delta settings, which facilitates storage and exchange of this data between Cisco Security Manager server instances.
VPN Configuration	
VPN wizard	Provides easy configuration of site-to-site, hub-and-spoke, full-mesh, and extranet VPNs.

Feature	Benefit
Support for common VPN deployment scenarios	Supports common VPN deployment scenarios with support for Group Encrypted Transport VPN (GET VPN), Dynamic Multipoint VPN (DMVPN), and generic routing encapsulation (GRE) IP Security (IPsec), both with dynamic IP and hierarchical certificates.
Multiple context configurations	Supports policy segmentation and flexibility with security configurations between different branch offices spanning. multiple locations.
Remote configuration	Centralizes the management of VPNs.
Efficiency and Usability Features	
Ticketing integration	Can tag changes made in multiple ticketing systems with a single ticket identifier, making them easily queried for audit.
Global search	Can find all devices, policies, and policy objects in the configuration database that use a particular IP address or service.
Find usage	Helps administrators quickly find usage information about objects by pointing to the exact rules that use a particular policy object, in addition to providing details about all the policies that use the object.
Auto-conflict detection	Provides a clear picture about rule conflicts to simplify rule optimization and troubleshooting.
IPv4 and IPv6 cross-compatibility	Supports configuration of unified IPv4 and IPv6 policies and rules to help speed up deployments and improve compatibility between policy configurations.
Integrated event management	Helps enable administrators to monitor status and troubleshoot security information, by providing: • Receipts of syslog messages from Cisco ASA appliances and Security Device Event Exchange (SDEE) messages from Cisco IPS sensors • Real-time and historical event views • Cross-linkages to firewall access rules and IPS signatures for quick navigation to the source policies • Prebundled sets of views for firewall, IPS, and VPN monitoring • Customizable views for monitoring select devices or a select time range • Intuitive GUI controls for searching, sorting, and filtering events • Administrative options to turn event collection on or off for select security devices • Launch of the Cisco Prime™ Security Manager when an ASA CX deployment is detected in the environment; this provides a way to manage CX via Cisco Security Manager
Report Manager	Supports system reports and the creation of predefined reports, all of which can be: • Viewed as charts and grids • Exported as PDF or Excel files • Scheduled for delivery by email • Scanned for more detail
Bulk operations	Reduces administrative overhead in networks that have a large number of devices. The feature includes: • Bulk import and export of policy objects • Bulk addition for offline devices • Bulk import of device-level overrides • Bulk automatic software image updates for all Cisco ASA appliances deployed throughout the network, providing a flexible, consistent, and faster way of deploying updates at scale
Device grouping	Allows administrators to create and define device groups based on business function or location, and then manage all devices in a group as a single device.
Policy Object Manager	Defines objects such as network addresses, services, device settings, time ranges, or VPN parameters once and then uses them any number of times to avoid manual entry of values.
Other Capabilities	
Third-party device support	Supports “unmanaged” endpoints and third-party devices.
Security services management	Manages integrated security services, including quality of service (QoS) for VPN, routing, and Cisco Network Admission Control (NAC).
Multiple application views	Provides multiple views into the application to support different use cases and experience levels.
Flexible deployment options	Can implement security deployments on either an on-demand or a scheduled basis.
Rollback	Can roll back deployments to a previous configuration if required.
Role-based access control	Defines and enforces up to five administrator roles; additional roles are available with the optional Cisco Secure Access Control Server (ACS).
Workflow	Can assign specific tasks to each administrator during the deployment of a policy, with formal change control and tracking.

Feature	Benefit
Distributed deployment	Includes the Auto Update Server and the Cisco Network Services Configuration Engine to simplify updates to large numbers of remote firewalls, which may have dynamic addresses or NAT addresses.
Integration with Cisco Cloud Web Security	Allows users to define rules on firewalls via Cisco Security Manager and gives an option to forward web traffic to Cisco Cloud Web Security.
Operational management	Includes CiscoWorks Resource Manager Essentials (RWAN) to assist with operational functions such as software distribution or device inventory reporting.
Health and performance monitoring	Continuously analyzes normal and clustered security environments and sends alerts when preset thresholds are reached.
IP Intelligence	Has embedded IP intelligence into several features. Users can look at value-added information such as FQDN and location information for an IP address from several widgets in the home screen such as Top Attackers and Top Victims, in the Report Manager while analyzing a specific chart, and in the Health and Performance Monitor. IP Intelligence also exists as a separate widget in itself that can be added to a dashboard.

Technical Specifications

Detailed hardware specifications and sizing guidelines for Cisco Security Manager are available at: http://www.cisco.com/go/csmanager.

Device Support

Table 3 summarizes the device product families supported by Cisco Security Manager. For a detailed list, including supported device software versions, see “Supported Devices and OS Versions for Cisco Security Manager” at: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Table 3. Overview of Cisco Devices Supported by Cisco Security Manager

Supported Devices
Cisco PIX Security Appliances
Cisco ASA 5500 Series and ASA 5500-X Series Adaptive Security Appliances
Cisco Integrated Services Routers (including 800, 1800, 2800, and 3800 Series)
Cisco Integrated Services Routers G2 (including 1900, 2900, and 3900 Series)
Cisco ASR 1000 Series Aggregation Service Routers
Cisco 7600 Series Routers
Cisco 7500 Series Routers
Cisco 7300 Series Routers
Cisco 7200 Series Routers
Cisco 7100 Series Routers
Cisco 3200 Series Routers
Cisco 2600 Series Routers
Cisco Catalyst 6500 Series Firewall Services Modules (FWSMs)
Cisco Catalyst 6500 Series VPN Services Modules (VPNSMs)
Cisco 7600 Series/Catalyst 6500 Series IPsec VPN Shared Port Adapters (VPN SPAs)
Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM-2)
Cisco IPS 4200 Series Sensors
Cisco AIP-SSM for Cisco ASA 5500 Series
Cisco AIP-SSC for Cisco ASA 5500 Series
Cisco IPS AIM for Integrated Services Routers
Cisco IPS Module for Access Routers Network Module - Cisco Intrusion Detection System (NM-CIDS)
Cisco Catalyst 3550, 3560, 3560E, 3750, 3750 Metro, and 4500 Series Switches; and Cisco Catalyst 4948 and 4948 10 Gigabit Ethernet Switches

Ordering Information

The Cisco Security Manager product bulletin describes the licensing options and ordering details. The bulletin is published at: http://www.cisco.com/go/csmanager.

The latest version of Cisco Security Manager that can be ordered is version 4.7

Cisco Services

Cisco takes a lifecycle approach to services and, with its partners, provides a broad portfolio of security services so enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

Cisco Services can help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, visit: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html.

- **Cisco Security Intelligence Operations (SIO)** provides a central location for early warning threat and vulnerability intelligence and analysis, Cisco IPS signatures, and mitigation techniques. Visit and bookmark Cisco SIO at: http://www.cisco.com/security.
- **Cisco Security IntelliShield Alert Manager Service** provides a customizable, web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.
- **Cisco Software Application Support (SAS) Service** keeps Cisco Security Manager up and running with around-the-clock access to technical support and software updates.
- **Cisco Security Optimization Service** helps organizations maintain peak network health. The network infrastructure is the foundation of an agile and adaptive business. The Cisco Security Optimization Service supports the continuously evolving security system to meet ever-changing security threats through a combination of planning and assessments, design, performance tuning, and ongoing support for system changes.

Cisco Security Manager software is eligible for technical support service coverage under the Cisco Software Application Support (SAS) service agreement, which features:

- Unlimited access to the Cisco Technical Assistance Center (TAC) for award-winning support. Technical assistance is provided by Cisco software application experts trained in Cisco security software applications. Support is available 24 hours a day, 7 days a week, 365 days a year, worldwide.
- Registered access to Cisco.com, a robust repository of application tools and technical documents to assist in diagnosing network security problems, understanding new technologies, and staying current with innovative software enhancements. Utilities, white papers, application design data sheets, configuration documents, and case management tools help expand your in-house technical capabilities.
- Access to application software bug fixes and maintenance, and minor software releases.

For More Information

For more information about Cisco Security Manager, visit http://www.cisco.com/en/US/products/ps6498/index.html or contact your account manager or a Cisco Authorized Technology Provider. You may also send an email to ask-csmanager@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-730892-01 08/14