White Paper

Cisco Security Manager: Upgrade to a 4.X Version for New Reporting, Monitoring, Analysis, and Other Features

What You Will Learn

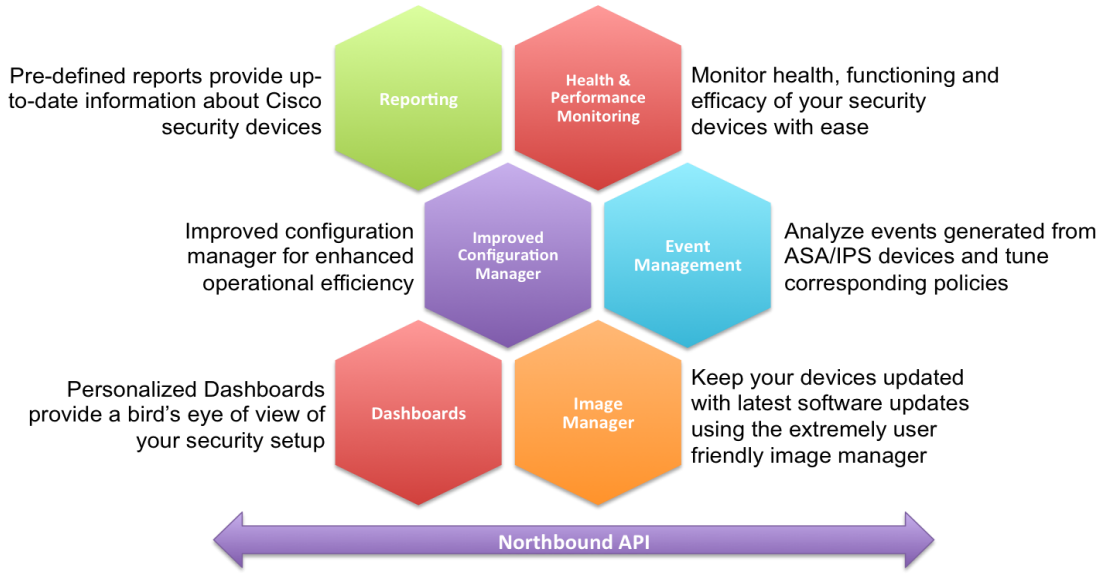
Cisco Security Manager is a powerful yet easy-to-use solution that is used to central provision all aspects of device configuration and security policies for Cisco firewalls, virtual private networks (VPNs), and Intrusion Prevention Systems (IPSs). The solution effectively manages even small networks consisting of fewer than 10 devices but can scale to efficiently manage large-scale networks with thousands of devices. For those using earlier releases of Cisco Security Manager, the recent 4.X releases provide many compelling reasons to upgrade based on a variety of beneficial features that are outlined in this white paper.

Overview

Over the years, Cisco Security Manager has evolved from being a policy management application to a full-fledged security management suite. Now the product's 4.x versions not only help with device configuration, but also support security experts in device monitoring for heath and efficacy, provide device-level security reporting, and make it easier to maintain the latest software and security updates. If you are currently using the 3.x series of Cisco Security Manager, you will find the latest version full of new and helpful features (Figure 1) to assist you in managing your security operations.

Cisco Security Manager is a comprehensive security management solution that is designed to manage several security devices simultaneously with ease. Through various management functions and a user-friendly interface, Cisco Security Manager makes security operations management more efficient and contributes to more informed policy decisions.

Figure 1. Cisco Security Manager Features Introduced in 4.x Releases



The following sections summarize the features that have been added in the recent 4.x releases

Improved Configuration Manager

Cisco Security Manager's configuration manager has improved dramatically since 3.x. Several features have been added to simplify policy management and improve operational efficiency. Auto-conflict detection is one such feature that enables maintaining a clean and effective policy table. The auto-conflict detection process has the capability to run through a huge number of policies that have been configured over time in Cisco Security Manager and identify the redundant rules that can then be deleted. Policy bundling is another feature that makes sharing of policies across hundreds of devices a very easy task. Users can group multiple policies into a bundle and the bundle can then be assigned to hundreds of devices at one go. Similarly, several other features have been added since 3.x that help in managing the latest Cisco Security devices effectively.

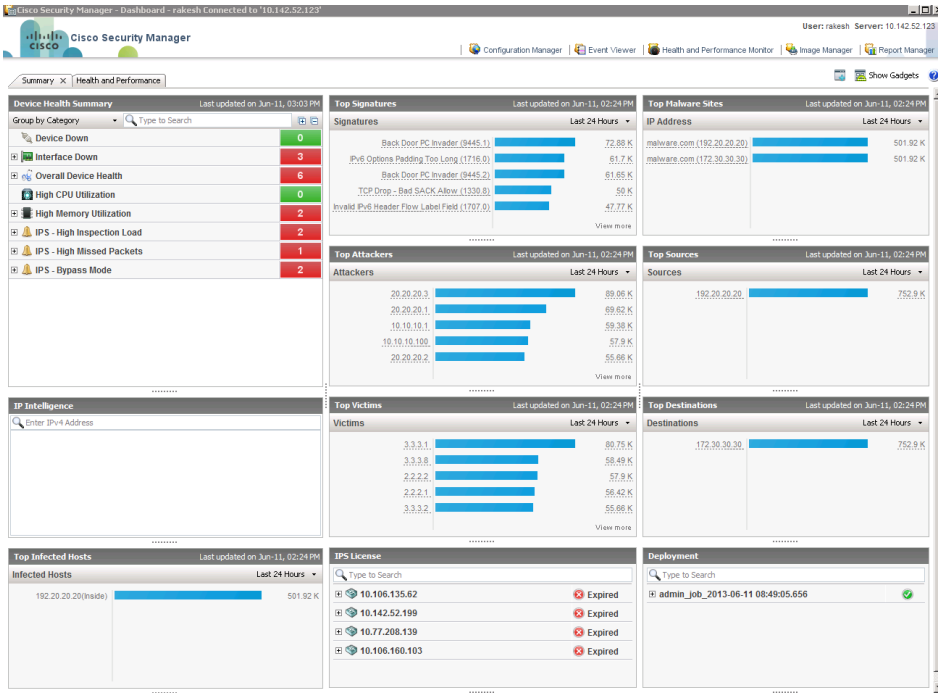
Figure 2. Cisco Security Manager: Auto Conflict Detection

Dashboard

The Cisco Security Manager dashboard 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 device

health summary, top attackers, top victims, top signatures and many more such widgets, provide an excellent summary of what an administrator needs to be and need not be concerned about. These widgets act as a starting point for any analysis. For example, in the Signatures widget, a user can click on 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, one can click on an IP address on the top attackers widget and look at value added information related to that IP address. So in effect, the dashboard screen is the starting point for security administrators on Cisco Security Manager. Additionally, these dashboards can be personalized to suit each user's needs.

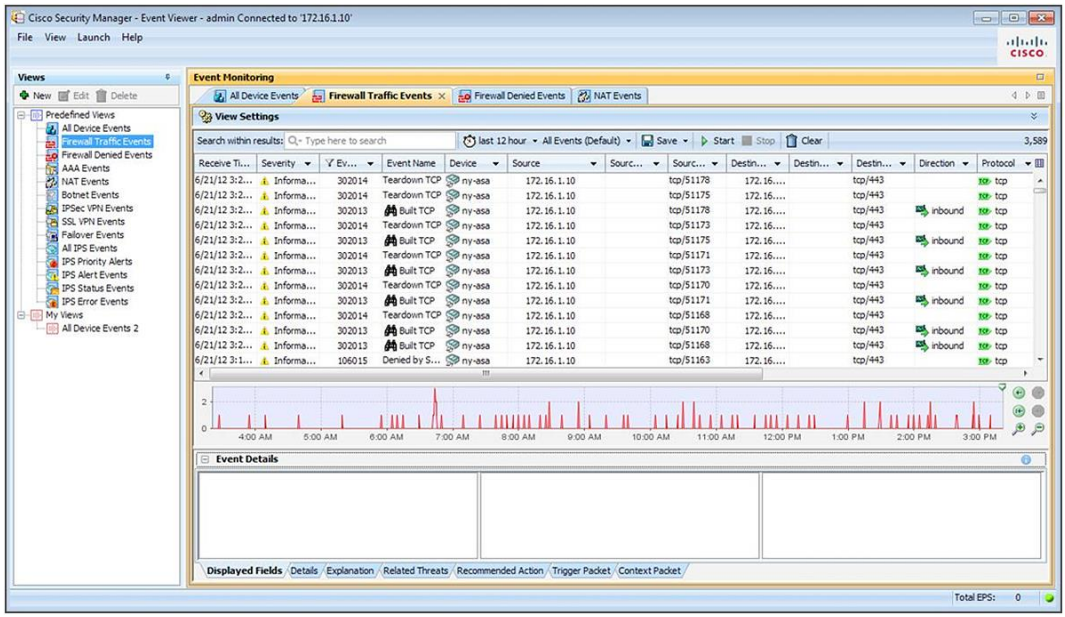
Figure 3. Cisco Security Manager Dashboard



Event Management and Troubleshooting

Integrated event management helps enable viewing of real-time and historical events for rapid incident analysis and troubleshooting, and provides rapid navigation from events to source policies. In addition, advanced filtering and search capabilities enable administrators to quickly identify and isolate interesting events. Cross-linkages between the Event Manager and Configuration Manager reduce troubleshooting time for firewall rules, as well as for IPS signatures (see Figure 4).

Figure 4. 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

Reporting

Cisco Security Manager (Figure 5) generates detailed system reports based on events and other essential information gathered from throughout the security deployment. 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 drill down from a specific chart to view additional information for further analysis.

Figure 5. Report Manager in Cisco Security Manager

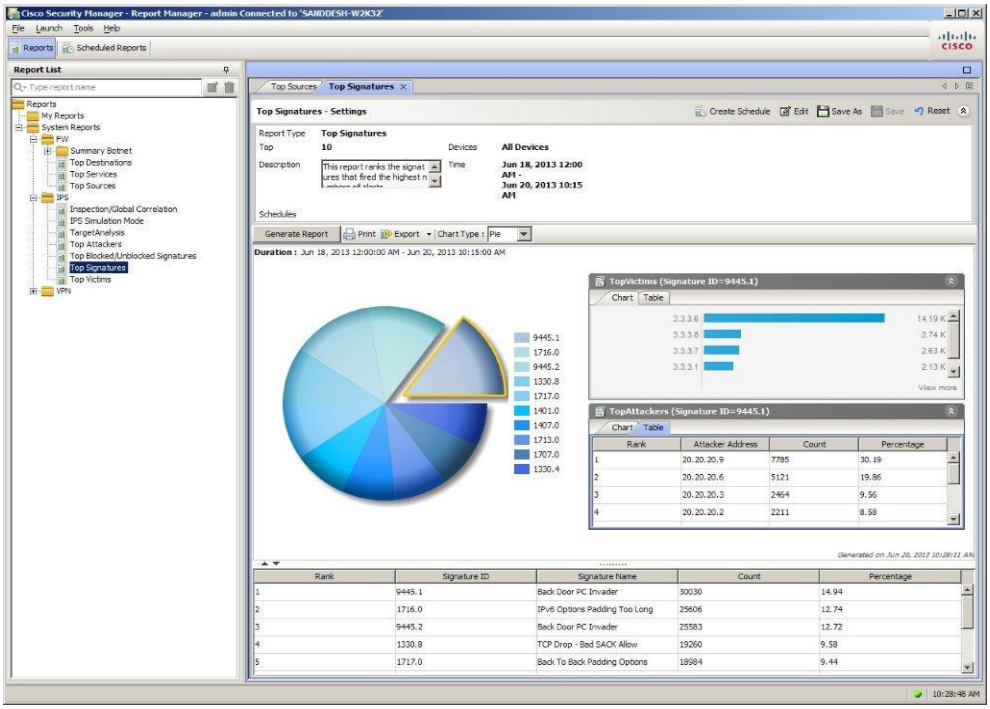


Table 1. Cisco Security Manager System Reports

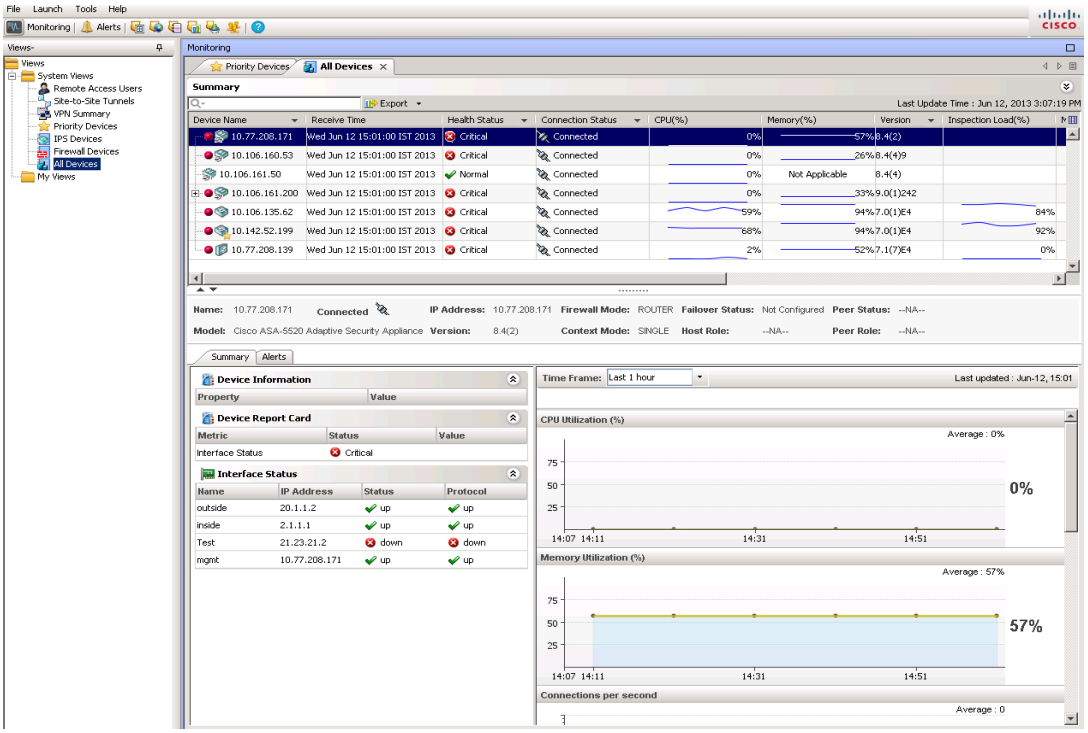
Firewall	IPS	VPN
• Top Infected Hosts • Top Malware Ports • Top Malware Sites • Top Destinations • Top Services • Top Sources	• Inspection/Global Correlation • IPS Simulation Mode • Target Analysis • Top Attackers • Top Blocked/Unblocked Signatures • Top Signatures • Top Victims	• Top Bandwidth Users (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 (for example, CPU or memory utilization) 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 health, traffic, and performance metrics of each device, as desired. Figure 6 shows the primary monitoring interface.

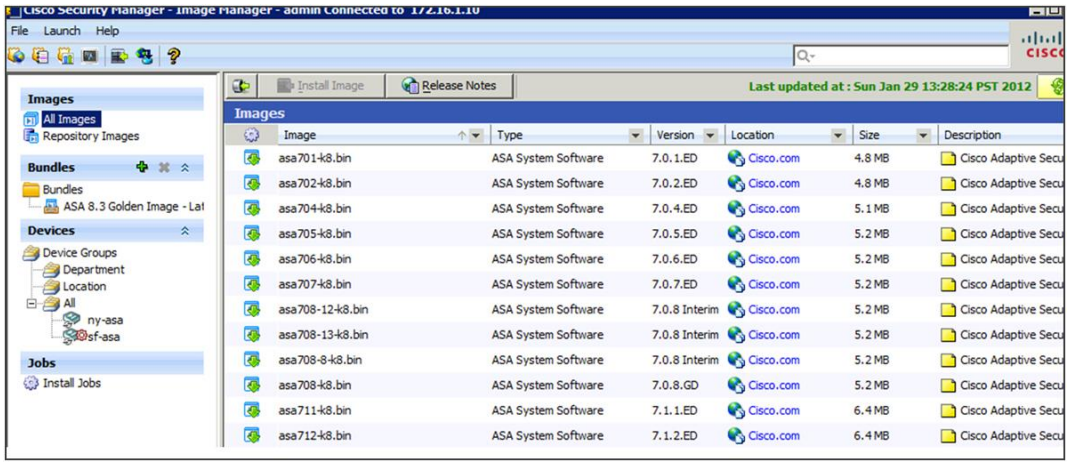
Figure 6. Health and Performance Monitor in Cisco Security Manager



Software Image Upgrade

Firewall software images can be upgraded using an intuitive wizard. The wizard will lead administrators through the steps required to download the images, create the image bundle, and ensure that the image is appropriate for each device. The tool will then perform the backup, take the devices down, and perform the update. The updates can be performed on each firewall individually, or updates can be run in groups to maximize speed and efficiency. The process is automated, so it can be run overnight or during noncritical times to minimize disruption to the operating environment. Figure 7 shows the primary image management interface of Cisco Security Manager.

Figure 7. Software Image Upgrade in Cisco Security Manager



API-Based Access to Cisco Security Manager

API-based access enables Cisco Security Manager to securely share information with other essential network services such as compliance and advanced security analysis systems to streamline their security operations and compliance. Using representational state transfer, external firewall compliance systems can directly request access to data from any security device managed by Cisco Security Manager.

Technical Specifications

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

Device Support

For a detailed list of supported devices and 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.

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.

Two product packages are available:

- Cisco Security Manager Standard Edition
- Cisco Security Manager Professional Edition

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 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 C11-731704-00 05/14