Cisco Security Manager 4.4

Q. What is Cisco Security Manager?

A. Cisco® Security Manager is a comprehensive management solution that enables advanced management and rapid troubleshooting of multiple security devices. Cisco Security Manager provides scalable, centralized management from which administrators can efficiently manage a wide range of Cisco security devices, gain visibility across the network deployment, and securely share information with other essential network services such as compliance systems and advanced security analysis systems. Designed to maximize 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 of trouble tickets.

Q. Who should deploy Cisco Security Manager?

A. Cisco Security Manager is designed to meet the security management needs of small to large enterprise environments that employ Cisco security devices. Cisco Security Manager supports a wide range of Cisco security devices, including Cisco ASA 5500 Series adaptive security appliances, Cisco IPS 4200 and 4300 Series sensors, Cisco Secure Routers, and the Cisco AnyConnect® Secure Mobility Client.

Q. What's new in Cisco Security Manager 4.4?

A. Cisco Security Manager 4.4 provides several enhancements. Major new features in this release include:

- Management of ASA clusters, so you can view multiple ASA appliances together as a single logical device.
- Health and performance monitoring of Cisco ASA cluster and regular configurations and IPS configurations provides a continuous analysis of the security environment and sends alerts when preset thresholds are reached.
- Cisco TrustSec® Security Group Tags can be used in Cisco Security Manager to create granular and highly optimized security policies that can be deployed at scale through the security infrastructure.
- Ability to create unified IPv4 and IPv6 policies speeds up configuration deployments and helps reduce overhead of multiple policy configurations.
- Advanced VPN capabilities allow multiple context configurations to provide policy segmentation and flexibility with security configurations between different branch offices and locations.
- Integration with ScanSafe (Cisco Cloud Web Security) through a connector allows users to define rules on firewalls that can forward web traffic to the ScanSafe cloud.
- API-based access for Cisco Security Manager policy configuration data enables organizations to securely share information with other applications for compliance and advanced security analysis.
- Administrative overhead is reduced in networks with a large number of devices. Ticketing integration enables changes made in multiple ticketing systems to be easily queried for audit.
- A variety of efficiency and usability features, including global search of devices, policies, and policy objects; search of usage information about objects; auto-conflict detection; policy object management; and support for Cisco ASA 5500-X Series midrange security appliances and Cisco IPS 4300 Series sensors.

Q. What are the new clustering management capabilities available in Cisco Security Manager?

A. The clustering feature provides an efficient way to scale the throughput of a group of ASAs by having them all work in concert to pass connections as one logical ASA device. Using up to eight ASA appliances, clustering scales to 100 Gbps of aggregate traffic through the cluster. ASA clustering provides advanced failover capabilities and a load-sharing mechanism to reduce downtime and improve availability. Clustering supports single and multiple contexts, as well as routed and transparent modes. Cisco Security Manager allows users to view and monitor each cluster as a single entity, and maintains the same configuration across all units in the cluster using automatic configuration sync. Events coming from the cluster are processed for troubleshooting, and health and performance statistics of clusters are also provided to track resource usage.

Q. What are the benefits of the integration with Cisco TrustSec Security Group Tags?

A. Integration with Cisco TrustSec Security Group Tags enables Cisco Security Manager users to configure granular and highly relevant policies across conventional as well as clustering deployments. The information from the Security Group Tags is used to optimize and deploy consistent policies, which helps increase operational efficiencies and decrease operational expenses. The benefits of this integration are:

- Policy stays with the user/server, regardless of access location.
- Firewall access and control administration can easily be automated via Cisco Security Manager.
- ACL maintenance, complexity, and overhead is highly reduced, which makes security management simpler and more efficient.
- Security rules and policies are easier to audit and optimize.

Q. What are the image management capabilities?

A. Cisco Security Manager provides the capability to upgrade firewall software images directly using an intuitive wizard, instead of with CiscoWorks Resource Manager Essentials (RME). A software image repository enables images to be imported from Cisco's online software website or from the local file system. Using software bundling, downloaded images that are tested to be "good" can be grouped together such that all subsequent device upgrades can use the validated image set. All image deployments validate whether the devices have enough storage space for the new images. Cisco Security Manager understands the firewall failover pairs and deploys to the pair in a sequential manner to help ensure that either the primary or the failover device is up at all times during the upgrade process. 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.

Q. What are the health and performance monitoring capabilities of Cisco Security Manager?

A. Cisco Security Manager 4.3 introduced new capabilities to monitor health and performance of firewalls, intrusion prevention systems (IPSs), and VPNs. A simple color-coded interface enabled quick identification of the devices that are in critical condition. Integrated sparkline charts for commonly monitored attributes (CPU, memory utilization, and so on) enable rapid identification of the health and performance trends of all the devices. Detailed charts can be used to get more information about health, traffic, and performance metrics of the devices.

Cisco Security Manager 4.4 now provides health and performance monitoring that goes beyond the previous capabilities to support clustering environments as well.

Q. What are the API capabilities?

A. 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. Several security compliance vendors, including Tufin, Algosec, and Skybox, have updated their products to work with the new APIs in Cisco Security Manager.

Q. What kind of training is available for Cisco Security Manager 4.4?

A. Visit http://www.cisco/com/go/csmanager for Cisco Security Manager 4.4 data sheets, bulletins, and deployment guides. In addition, Cisco will provide a new learning course, as well as related online videos and webinars.

Q. What is the upgrade path for existing Cisco Security Manager customers?

A. Existing Cisco Security Manager 4.X customers with valid software support can obtain an upgrade to Cisco Security Manager 4.4. Customers with Version 3.X will first need to upgrade to Cisco Security Manager 4.0 by purchasing Cisco Security Manager 4.0 upgrade licenses. There is no direct upgrade path from Cisco Security Manager 3.X to Cisco Security Manager 4.4. The upgrade procedure from Cisco Security Manager 3.X to Cisco Security Manager 4.0 is covered in the Cisco Security Manager 4.0 Product Bulletin.

Q. Is Cisco Security Manager 4.4 supported on VMware?

A. Yes. Cisco Security Manager 4.4 is supported on VMware ESX/ESXi Server 5.0.

Q. Does Cisco Security Manager 4.4 support Cisco ASA CX Context-Aware Security?

A. Cisco Security Manager 4.4 does not manage Cisco ASA CX Context-Aware Security on its own, but it launches Cisco Prime™ Security Manager (which manages Cisco ASA CX Context-Aware Security) when CX deployment is detected in the environment, thereby providing a basic path to manage CX via Cisco Security Manager.

Q. What support options are available for Cisco Security Manager?

A. Cisco Security Manager is eligible for technical support service coverage under Cisco Software Application Support (SAS).

For details on Cisco SAS coverage, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2993/serv_group_home.html.

Cisco Software Application Support plus Upgrades (SASU) is not available for Cisco Security Manager.

Q. What options are available to evaluate Cisco Security Manager?

A. Anybody with a valid Cisco.com account can download Cisco Security Manager and use the software for up to 90 days in evaluation mode. Visit http://www.cisco.com/go/csmanager and select the Download Software link.

Note: This download does not include CiscoWorks Resource Manager Essentials (RME).

Q. Where can I find a technical Q&A for Cisco Security Manager?

A. An updated version of the “FAQs and Troubleshooting Guide for Cisco Security Manager 4.X” is available at: http://www.cisco.com/en/US/products/ps6498/prod_troubleshooting_guides_list.html.

For specific recommendations on deploying Cisco Security Manager, download the latest deployment guide at: http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

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 C67-727089-00 03/13