Cisco Security Manager 4.2: Integrated Security Management for Cisco Firewall, IPS, and VPN Solutions

Security Operations Challenges

Businesses are facing daunting new challenges in security operations. A growing number of security technologies, combined with the reduction and redirection of IT headcount once dedicated to security management, has resulted in a challenging operational environment. Security professionals have been stretched to the point where human error now frequently results in security exposure and incidents. Integrated end-to-end tools that enable consistent policy enforcement and quick troubleshooting of security events, in addition to providing summarized reports about the security deployment, are invaluable to operations teams.

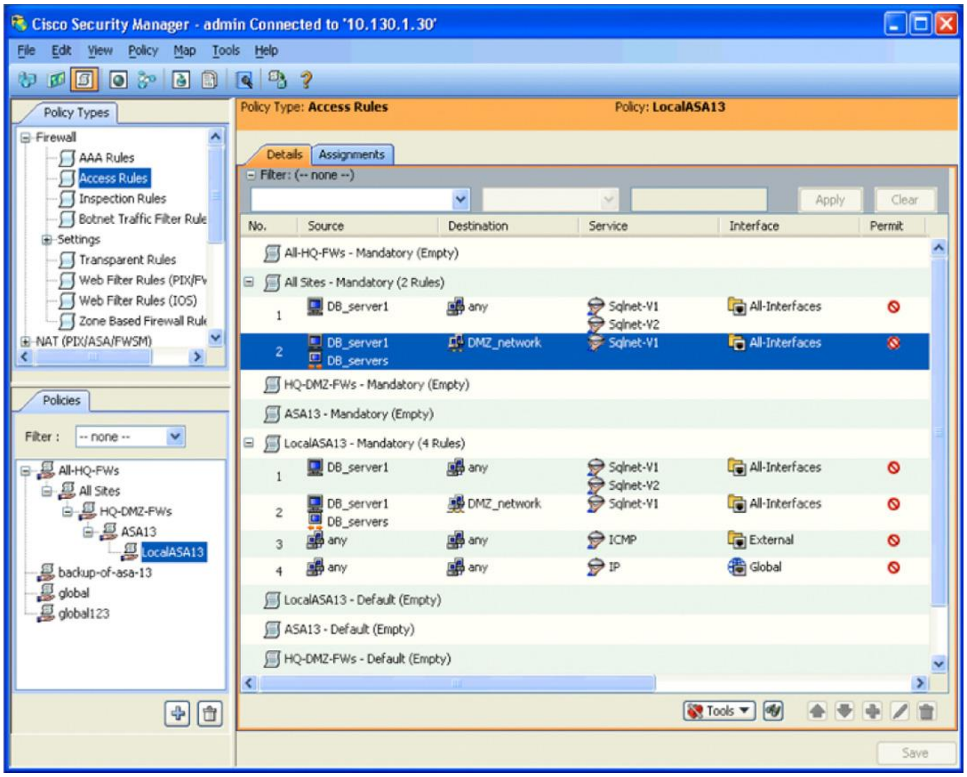
Cisco Security Manager Overview

Cisco® Security Manager enables enterprises to manage and scale security operations efficiently and accurately. Cisco Security Manager integrates a powerful suite of capabilities, including policy and object management, event management, reporting, and troubleshooting, which are essential to maintaining security posture in today's ever-changing threat environment. Cisco Security Manager supports a range of security solutions, including Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IPS 4200 Series Sensor Appliances, Cisco Secure Routers, and the Cisco AnyConnect™ Secure Mobility Client.

Security Policy Management

Security administrators can create reusable network objects such as network addresses and services, which are defined once and used any number of times. Cisco Security Manager also allows policies to be defined once and shared across devices. This minimizes errors associated with manual entry of data, and makes the management of security objects and policies more efficient. Administrators can implement both on-demand and scheduled security deployments, 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 1.

Figure 1. Security Policy Management



No.	Source	Destination	Service	Interface	Permit
All-HQ-FWs - Mandatory (Empty)					
All Sites - Mandatory (2 Rules)					
1	DB_server1	any	Sqlnet-V1 Sqlnet-V2	All-Interfaces	⊘
2	DB_server1 DB_servers	DMZ_network	Sqlnet-V1	All-Interfaces	⊘
HQ-DMZ-FWs - Mandatory (Empty)					
ASA13 - Mandatory (Empty)					
LocalASA13 - Mandatory (4 Rules)					
1	DB_server1	any	Sqlnet-V1 Sqlnet-V2	All-Interfaces	⊘
2	DB_server1 DB_servers	DMZ_network	Sqlnet-V1	All-Interfaces	⊘
3	any	any	ICMP	External	⊘
4	any	any	IP	Global	⊘
LocalASA13 - Default (Empty)					
ASA13 - Default (Empty)					
HQ-DMZ-FWs - Default (Empty)					

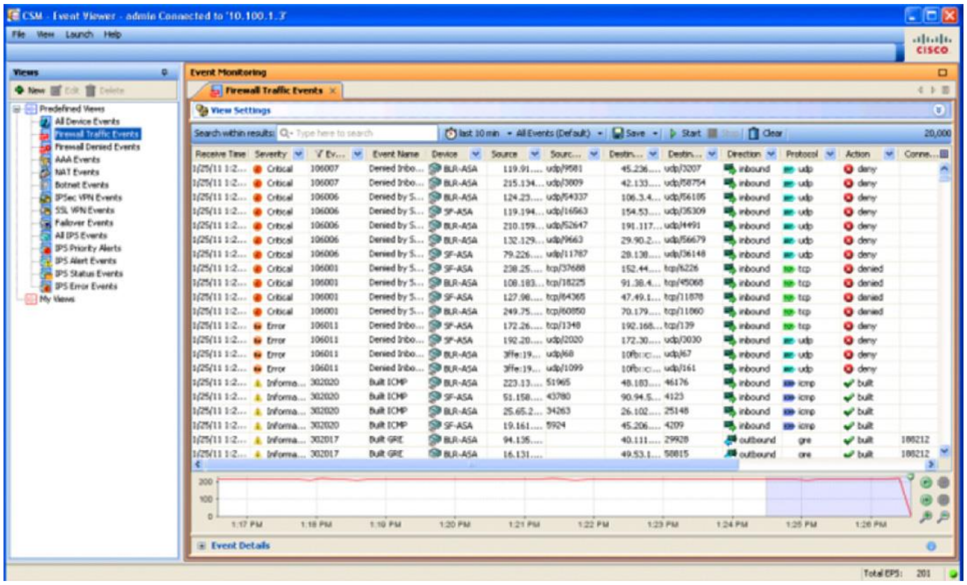
Cisco Security Manager also enables flexible provisioning of IPS signature updates, providing administrators with the ability to incrementally provision new and updated signatures, create IPS policies for those signatures, and then share the policies across devices. Additionally, insight into Cisco Security Intelligence Operations (SIO) recommendations allows administrators to fine-tune their environment prior to deploying signature updates. The following features allow security teams to significantly cut the amount of time spent on manual tasks while reducing errors and optimizing their security environment:

- Policy and object sharing enables security rules and objects to be reused.
- RBAC and workflow ensure error-free deployments and process compliance.
- Flexible deployments and rollback capabilities provide administrators the tools to efficiently implement defined policies.
- Provisioning of IPS signature updates and access to Cisco SIO enhance the ability of security teams to keep up with ever-growing security threats.

Event Management and Troubleshooting

Integrated event management provides administrators with real-time incident analysis and rapid troubleshooting, while advanced filtering and search capabilities enable them to quickly identify and isolate interesting events. Cross-linkages between the event manager and configuration manger reduce troubleshooting time for firewall rules and IPS signatures. See Figure 2.

Figure 2. Event Management and Troubleshooting



Receive Time	Severity	Ev...	Event Name	Device	Source	Sourc...	Destin...	Destin...	Direction	Protocol	Action	Conne...
1/25/11 1:2...	Critical	106007	Denied Inbo...	BLR-ASA	119.91....	udp/9581	45.236....	udp/3207	inbound	udp	deny	
1/25/11 1:2...	Critical	106007	Denied Inbo...	BLR-ASA	215.134...	udp/3809	42.133....	udp/58754	inbound	udp	deny	
1/25/11 1:2...	Critical	106006	Denied by S...	BLR-ASA	124.23....	udp/54337	106.3.4...	udp/56105	inbound	udp	deny	
1/25/11 1:2...	Critical	106006	Denied by S...	SF-ASA	119.194...	udp/16563	154.53....	udp/35309	inbound	udp	deny	
1/25/11 1:2...	Critical	106006	Denied by S...	BLR-ASA	210.159...	udp/52647	191.117...	udp/4491	inbound	udp	deny	
1/25/11 1:2...	Critical	106006	Denied by S...	BLR-ASA	132.129...	udp/9663	29.90.2...	udp/56679	inbound	udp	deny	
1/25/11 1:2...	Critical	106006	Denied by S...	SF-ASA	79.226....	udp/11787	28.138....	udp/36148	inbound	udp	deny	
1/25/11 1:2...	Critical	106001	Denied by S...	SF-ASA	238.25....	tcp/37688	152.44....	tcp/6226	inbound	tcp	denied	
1/25/11 1:2...	Critical	106001	Denied by S...	BLR-ASA	108.183...	tcp/18225	91.38.4...	tcp/45068	inbound	tcp	denied	
1/25/11 1:2...	Critical	106001	Denied by S...	SF-ASA	127.98....	tcp/64365	47.49.1...	tcp/11878	inbound	tcp	denied	
1/25/11 1:2...	Critical	106001	Denied by S...	BLR-ASA	249.75....	tcp/60850	70.179....	tcp/11860	inbound	tcp	denied	
1/25/11 1:2...	Error	106011	Denied Inbo...	SF-ASA	172.26....	tcp/1348	192.168...	tcp/139	inbound	tcp	deny	
1/25/11 1:2...	Error	106011	Denied Inbo...	SF-ASA	192.20....	udp/2020	172.30....	udp/3030	inbound	udp	deny	
1/25/11 1:2...	Error	106011	Denied Inbo...	BLR-ASA	3ffe:19...	udp/68	10fb::c...	udp/67	inbound	udp	deny	
1/25/11 1:2...	Error	106011	Denied Inbo...	BLR-ASA	3ffe:19...	udp/1099	10fb::c...	udp/161	inbound	udp	deny	
1/25/11 1:2...	Informa...	302020	Built ICMP	BLR-ASA	223.13....	51965	48.183....	46176	inbound	icmp	built	
1/25/11 1:2...	Informa...	302020	Built ICMP	SF-ASA	51.158....	43780	90.94.5...	4123	inbound	icmp	built	
1/25/11 1:2...	Informa...	302020	Built ICMP	BLR-ASA	25.65.2...	34263	26.102....	25148	inbound	icmp	built	
1/25/11 1:2...	Informa...	302020	Built ICMP	SF-ASA	19.161....	5924	45.206....	4209	inbound	icmp	built	
1/25/11 1:2...	Informa...	302017	Built GRE	BLR-ASA	94.135....		40.111....	29928	outbound	gre	built	188212
1/25/11 1:2...	Informa...	302017	Built GRE	BLR-ASA	16.131....		49.53.1...	58815	outbound	gre	built	188212

The Cisco Security Manager Event Viewer provides:

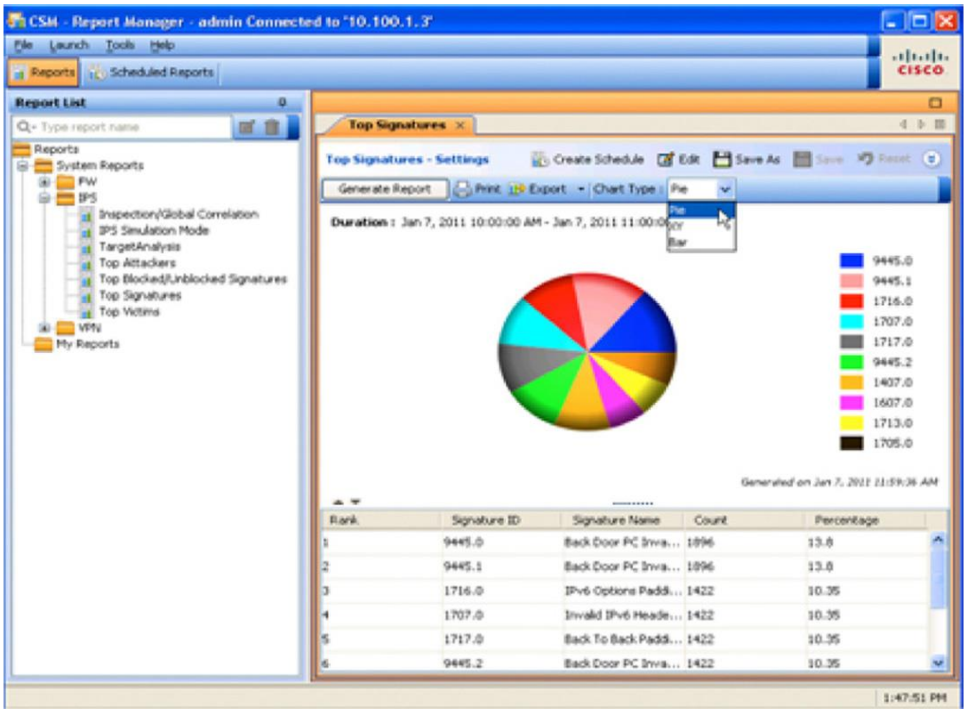
- Support for syslog messages created by Cisco ASA appliances, Cisco Firewall Services Modules (FWSMs), and Security Device Event Exchange (SDEE) messages from Cisco IPS sensors
- Real-time and historical event viewing
- Cross-linkages to firewall access rules and IPS signatures, for quick navigation to the source policies
- A pre-bundled 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 multi-vendor environments, event correlation, and historical event analysis is available at http://www.cisco.com/go/securitypartners.

Reporting

Cisco Security Manager 4.2 includes a report manager, which generates system reports from events that it receives and displays them as either charts or data grids. It also allows administrators to define and save custom reports using advanced report criteria to meet their specific reporting needs. All report data and charts can be exported to PDF and Excel, and they can be scheduled for email delivery as PDF or CSV files. See Figure 3 and Table 1 for a list of system reports.

Figure 3. Reporting



CSM - Report Manager - admin Connected to '10.100.1.3'

Duration : Jan 7, 2011 10:00:00 AM - Jan 7, 2011 11:00:00

Generated on Jan 7, 2011 11:59:36 AM

Rank	Signature ID	Signature Name	Count	Percentage
1	9445.0	Back Door PC Inva...	1896	13.8
2	9445.1	Back Door PC Inva...	1896	13.8
3	1716.0	IPv6 Options Paddi...	1422	10.35
4	1707.0	Invalid IPv6 Heade...	1422	10.35
5	1717.0	Back To Back Paddi...	1422	10.35
6	9445.2	Back Door PC Inva...	1422	10.35

1:47:51 PM

Table 1. 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

Cisco Security Manager Use Cases

Table 2 describes the primary use cases for Cisco Security Manager.

Table 2. Cisco Security Manager Primary Use Cases

Feature	Benefit
Firewall Management	• Powerful object and rule sharing capabilities enable administrators to efficiently and consistently maintain their firewall estate • Innovative policy query feature displays which rules match a specific source, destination, and service flow, including wildcards; this feature allows the administrator to define policies more efficiently • To ease configuration, device information can be imported from a device repository or configuration file, or added in the software; additionally, firewall policies can be discovered from the device itself - this feature simplifies initial security management setup • Consumption of ASA/ASASM/FWSM syslog events • System-generated and customized reports, including firewall traffic and botnet reports

Feature	Benefit
IPS Management	- Incremental provisioning of new and updated signatures - Insight into Cisco SIO recommended defaults allows customers to tune their environment before distributing the signature update - IPS signature policies and event action filters can be inherited and assigned to any device - all other IPS polices can be assigned to and shared with other IPS devices; IPS management also includes policy rollback, a configuration archive, and cloning or creation of signatures - IPS update administration and IPS subscription licensing updates allow users to manage IPS software, signature updates, and licensing based on local and shared polices - Consumption and viewing of IPS SDEE events - System and custom IPS reports, including top attackers, top signatures
Site-to-Site VPN Management	- Easy configuration of site-to-site, hub-and-spoke, full-mesh, and extranet VPNs - Support for Group Encrypted Transport VPN (GET VPN), Dynamic Multipoint VPN (DMVPN), and Generic Routing Encapsulation (GRE) - Support for a variety of site-to-site IPsec VPN configurations, including dynamic IP, hierarchical certificates, and preshared keys - Extranet IPsec VPN support for establishing tunnels to partner networks and third-party devices
Cisco AnyConnect Management	- Enables large scale Cisco AnyConnect deployments via policy sharing across multiple ASA appliances - Supports advanced configurations of Cisco Secure Desktop - Provisioning of IPsec Remote Access and SSL VPNs - Multiple system reports tailored for remote access administration

Technical Specifications

For more information on Cisco Security Manager hardware and software requirements, see the Cisco Security Manager Deployment Guide 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 4.2" at http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

Table 3. Highlights of Security Solutions Supported by Cisco Security Manager

Device Support Highlights
Cisco ASA 5500 Series Adaptive Security Appliances
Cisco IPS Sensors
Cisco Catalyst 6500 Series Firewall Services Modules (FWSMs)
Cisco AnyConnect Secure Mobility Client
Cisco Integrated Services Routers
Cisco 1000 Series Aggregation Service Routers (ASRs)

Ordering Information

A summary of licensing options is provided in Table 4. For complete ordering details, please refer to the Cisco Security Manager 4.2 Product Bulletin at http://www.cisco.com/go/csmanager.

Table 4. Summary of Licensing Options for Cisco Security Manager 4.2

Cisco Security Manager Standard Edition	
L-CSMST5-4.2-K9	Cisco Security Manager 4.2 Standard - 5 Device Limit
L-CSMST10-4.2-K9	Cisco Security Manager 4.2 Standard - 10 Device Limit
L-CSMST25-4.2-K9	Cisco Security Manager 4.2 Standard - 25 Device Limit

Cisco Security Manager Professional Edition	
L-CSMPR50-4.2-K9	Cisco Security Manager 4.2 Professional with 50 Device License
L-CSMPR100-4.2-K9	Cisco Security Manager 4.2 Professional with 100 Device License
L-CSMPR250-4.2-K9	Cisco Security Manager 4.2 Professional with 250 Device License
Cisco Security Manager Incremental Device Licenses	
L-CSMPR-LIC-50	Cisco Security Manager Pro - Incremental 50 Device License
L-CSMPR-LIC-100	Cisco Security Manager Pro - Incremental 100 Device License
L-CSMPR-LIC-250	Cisco Security Manager Pro - Incremental 250 Device License

Note: The incremental device licenses are only available to customers who have bought the Professional Edition of Cisco Security Manager.

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.

- **Cisco Security Intelligence Operations (SIO) Service** provides a central location for early warning threat and vulnerability intelligence and analysis, Cisco IPS signatures, and mitigation techniques.
- **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 minor software releases.
- **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.

For More Information

For more information about Cisco Security Manager 4.2, visit http://www.cisco.com/go/csmanager or contact your account manager or a Cisco Authorized Technology Provider.

Related Products and Services

For more information about Cisco security solutions, please visit the links below:

- Cisco ASA 5500 Series Adaptive Security Appliances http://www.cisco.com/go/asa
- Cisco Intrusion Prevention Systems http://www.cisco.com/go/ips
- Cisco AnyConnect Secure Mobility Client http://www.cisco.com/go/anyconnect
- Cisco Security Intelligence Operations http://www.cisco.com/security
- Cisco Advanced Services for Security
http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.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

C78-687393-00 09/11