ılıılı cısco

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.

cisco Security Manager	Configuration	n Manager 🚑 Event Viewer	🍓 Health and Performance Monitor 🍓 I	User: rakesh Server: 10.142.52 mage Manager 🙀 Report Mana
Summary × Health and Performance				🔄 🧱 Show Gadgets
Device Health Summary Last updated on Jun-11, 03:03 P	M Top Signatures Last	updated on Jun-11, 02:24 PM	Top Malware Sites	Last updated on Jun-11, 02:24 P
Group by Category	3 Signatures	Last 24 Hours 👻	IP Address	Last 24 Hours
Na Device Down	Back Door PC Invader (9445.1)	72.88 K	malware.com (192.20.20.20)	501.92
E 🔤 Interface Down 3	IPv6 Options Padding Too Long (1716.0)	<u>61.7 K</u>	malware.com (172.30.30.30)	501.92
Overall Device Health G	Back Door PC Invader (9445.2)	61.65 K		
High CPU Utilization	TCP Drop - Bad SACK Allow (1330.8)	50 K		
High Memory Utilization	Invalid IPv6 Header Flow Label Field (1707.0)	47.77 K		
IPS - High Inspection Load 2		View more		
🔔 IPS - High Missed Packets	Top Attackers	updated on Jun-11, 02:24 PM	Top Sources	Last updated on Jun-11, 02:24 P
IPS - Bypass Mode 2	Attackers	Last 24 Hours +	Sources	Last updated on Jun-11, 02:24 P
	Attackers	Cast 24 Hours +	Sources	Last 24 Hours
	20.20.20.3	89.06 K	192.20.20.20	752.9
	20.20.20.1	69.62 K		
	<u>10.10.10.1</u> 10.10.100	59.38 K		
	20.20.20.2	57.9 K 55.66 K		
		View more		
		View more	· · · · · · · · · · · · · · · · · · ·	
IP Intelligence	Top Victims Last	updated on Jun-11, 02:24 PM	Top Destinations	Last updated on Jun-11, 02:24 P
CEnter IPv4 Address	Victims	Last 24 Hours 👻	Destinations	Last 24 Hours
	3.3.3.1	80.75 K	172.30.30.30	752.9
	3.3.3.8	58.49 K		
	2222	57.9 K		
	2.2.2.1	56.42 K		
	3.3.3.2	55.66 K		
		View more		
Top Infected Hosts Last updated on Jun-11, 02:24 P	M IP5 License		Deployment	
nfected Hosts Last 24 Hours			C Type to Search	
192.20.20.20(Inside) 501.92		🔞 Expired	■ admin_job_2013-06-11 08:49:05.65	6 🥑
		😢 Expired		
		🔞 Expired		
		S Expired		
		w copied		

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).

evices 🕂 🕆	Device: ny-as	sa		Policy: Access Rules			
ter : none	Policy Assigne	d: Global F	<u>W Policy</u> 5A Global FW-INS-BTF	Assigned To: 3 Devices	L	Inherits From: none	<u></u>
Department	+ Filter: (0006)					
- All	No.	Permit	Source	User	Destination	Service	Interface
- Store dc-asa			licy - Mandatory (23 Rules)),			
🚱 hq-ips 📯 la-asa	1	0	any any	, THREATDLABS\\Mktg	B DataCenter-1	PI 🚭	Global
- States	2	0	any any	THREATDLABS\\Mktg	DataCenter-2	PI 😪	Global
- 🕼 ny-asa-ssm	3	0	any any	THREATDLABS\\Mktg	DataCenter-3	PI 😴	Global
St@sf-asa	4	0	any any	THREATDLABS\\Mktg	CSM-Server	P IP	Global
	5	0	any any	THREATDLABS\\Br	DataCenter-1	P IP	Global
icies	6	0	any any	THREATDLABS\\Br	DataCenter-2	P IP	Global
Firewall	7	0	any any	THREATDLABS\\Br	DataCenter-3	DP IP	Global
AAA Rules	8	0	any any	THREATDLABS\\Br	CSM-Server	PI 😥	(B) Global
Access Rules	9	0	any any	THREATDLABS\\Engg	DataCenter-1	P IP	() Global
Inspection Rules	10	0	any any	THREATDLABS\\Engg	DataCenter-2	P IP	🔁 Global
Botnet Traffic Filter Rules	11	0	any any	THREATDLABS\\Engg	DataCenter-3	D IP	Global
-Settings	12	0	any any	THREATDLABS\\Engg	CSM-Server	P IP	Global
NAT	13	0	any any	no user	7.7.7.7	D IP	() Global
Site to Site VPN		~	any any	THREATDLABS\\Sa	8.8.8.8	DI IP	() Global
Remote Access VPN	S 15	~	Engineering_Net	THREATDLABS\\Engg	DataCenter-1	DP IP	Global
J Identity Options	S 16	~	Engineering_Net	THREATDLABS\\Engg	DataCenter-2	PI 😥	Global
Platform	- 17 (~	Engineering Net	THREATDLABS\\Enoo	DataCenter-3	el ⇔	Global ·

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

Predefined Vervs Al Device Events Predefined Vervs	ews ¢	Event Monitoring											
A Device Events Search within results: Q-Type here to search Source → Source → Sourc → Sourc → Destin	New 🛒 Edit 🏢 Delete	All Device Events	Firewall T	affic Events >	K 🚂 Firewa	I Denied Events 🛛 🐉 N	AT Events					4	4.0
Freedul Totific Sevents Search within results: Q- Type here to search Statt 12 hour < Al Events		View Settings											"
AAA Events Receive Tit Service Source	Firewall Traffic Events	Search within results: Q.+ Typ	e here to sear	ch	🐼 last 1	2 hour + All Events (De	fault) 🔹 🔛 S	ave - 🕨 St	tart 🔳 Stop 📋	Clear			3,
² / ₁ Mult Events ⁶ / ₁ /1/2 3:2 ¹ / ₁ forma ³ / ₁ 2014 ¹ / ₁ 22:2 ¹ / ₁ forma ³ / ₁ 22:1.6 ¹ / ₁ 12:2 ¹ / ₁ forma ³ / ₁ 22:1.6 ¹ / ₁ 12:2 ¹ / ₁ forma ³ / ₁ 22:1.6 ¹ / ₁ 12:2 ¹ / ₁ forma ³ / ₁ 22:1.6 ¹ / ₁ 12:2.6		Receive Ti Severity -	Y Ev •	Event Name	Device -	Source -	Sourc •	Sourc •	Destin • D	Destin • Destin •	Direction +	Protocol	
6 DSSc VPI Events 6/21/12 32 Informa 302013 4/4 buil TCP my-asa 172.1610 tcp/51178 172.16 tcp/443 mound		6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51178	172.16	tcp/443		tcp	
6 S1, VPF Events Fallower Events 6/21/12 32.2. 1 Informa 302014 Teardown TCP @ ny-asa 172.16.1.10 top/51173 172.16 top/443 18 inbound top P S Status Events 6/21/12 32.2. 1 Informa 302014 Teardown TCP @ ny-asa 172.16.1.10 top/51173 172.16 top/443 18 inbound 18 top P S Status Events 6/21/12 32.2. 1 Informa 302014 Teardown TCP @ ny-asa 172.16.1.10 top/51171 172.16 top/443 18 inbound 18 top P S Status Events 6/21/12 32.2. 1 Informa 302014 Teardown TCP @ ny-asa 172.16.1.10 top/51171 172.16 top/443 18 inbound 18 top P S Status Events 6/21/12 32.2. 1 Informa 302014 Teardown TCP @ ny-asa 172.16.1.10 top/51170 172.16 top/443 18 inbound 18 top M V Eve 19 S Status Events 2 6/21/12 32.2 1 Informa 302014 Teardown TCP @ ny-asa 172.16.1.10 top/51170 172.16 top/443 18 inb	Botnet Events	6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51175	172.16	tcp/443		top	
Palove Events 0/2/1/2.32 10mms 30013 1/2.16.1.10 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/3173 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 10/0/43 1/2.16 1/2.16 1/0/0/43 1/2.16 1/0/0/43 1/2.16 1/0/0/43 1/2.16 1/0/0/43 1/0/0/0/43 1/0/0/43 1/0/0/0/43<		6/21/12 3:2 1 Informa	302013	Buit TCP	S ny-asa	172.16.1.10		tcp/51178	172.16	tcp/443	inbound	top top	
M IDP Events 00/21/2 32.2 & Informa 302013 Textorin TCP Synyasa 1/2 16.1.10 ttp)511/3 1/2 16 ttp)43 ttp)400 fBP top PS Princty Verts PS Attrit Events 00/21/2 32.2 & Informa 302014 Textorion TCP Synyasa 1/2 16.1.10 ttp)511/3 1/2 16 ttp)443 ttp)400 fBP top PS Attrit Events PS Status Events 02/21/2 32.2 & Informa 302014 Textorion TCP Synyasa 1/2 16.1.10 ttp)511/3 1/2 16 ttp)443 ttp: top IPS Events PS Attrit Events PS Attrit Events 1/2 16.1.10 ttp)511/3 1/2 16 ttp)443 ttp: top ttp: top <td< td=""><td></td><td>6/21/12 3:2 1 Informa</td><td>302014</td><td>Teardown TCP</td><td>S ny-asa</td><td>172.16.1.10</td><td></td><td>tcp/51173</td><td>172.16</td><td>tcp/443</td><td></td><td>tcp</td><td></td></td<>		6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51173	172.16	tcp/443		tcp	
6/21/12 32: Informa 302014 Textdown TCP @ ny-ess 172.16.1.10 ttp/51171 172.16 ttp/443 Be too IPS Finity Alerts PS Xert Events 6/21/12 32: Informa 302014 Textdown TCP @ ny-ess 172.16.1.10 ttp/51171 172.16 ttp/443 Be too IPS Finity Alerts PS Xert Events 6/21/12 32: Informa 302014 Textdown TCP @ ny-ess 172.16.1.10 ttp/51170 172.16 ttp/443 Be too IPS Server Events 6/21/12 32: Informa 302014 Textdown TCP @ ny-ess 172.16.1.10 ttp/51170 172.16 ttp/443 Be too 6/21/12 32: Informa 302014 Textdown TCP @ ny-ess 172.16.1.10 ttp/51170 172.16 ttp/443 Be too 6/21/12 32: Informa 302013 ## built TCP @ ny-ess 172.16.1.10 ttp/51170 172.16 ttp/443 Be too 6/21/12 32: Informa 302013 ## built TCP @ ny-ess 172.16.1.10 ttp/51170 172.16		6/21/12 3:2 1 Informa	302013	Buit TCP	S ny-asa	172.16.1.10		tcp/51175	172.16	tcp/443	inbound 🖏	tep top	
By Salest Events 6/21/12 32 Informa 302013 ## built TCP Physics 172.1610 ttp/51173 172.16 ttp/443 We top M Vews IPS Fore Events 02013 ## built TCP Physes 172.16.1.10 ttp/51173 172.16 ttp/443 We top M Vews IPS Fore Events 02014 Teardown TCP Physes 172.16.1.10 ttp/51171 172.16 ttp/443 We top M Device Events 2 Informa		6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51171	172.16	tcp/443		top top	
DPS Status Events 6/2/1/2 32.2 informa 302014 Teardown TCP @ ny-asa 172.16.1.0 ttp/S1170 172.16 ttp/H43 180 top Al Device Events 2 6/2/1/2 32.2 informa 302014 Teardown TCP @ ny-asa 172.16.1.10 ttp/S1171 172.16 ttp/H43 180 top Al Device Events 2 6/2/1/2 32.2 informa 302013 Al Buit TCP @ ny-asa 172.16.1.10 ttp/S1171 172.16 ttp/H43 180 top 6/2/1/2 32.2 informa 302013 Al Buit TCP @ ny-asa 172.16.1.10 ttp/S1170 172.16 ttp/H43 180 top 6/2/1/2 32.2 informa 302013 Al Buit TCP @ ny-asa 172.16.1.10 ttp/S1170 172.16 ttp/H43 180 top 180 top 180 top 172.16.1.10 ttp/S1170 172.16 ttp/H43 180 top 172.16.1.10 ttp/S1163 172.16 ttp/H43 180 top 172.16.1.10 ttp/S1163 172.16		6/21/12 3:2 1 Informa	302013	Buit TCP	S ny-asa	172.16.1.10		tcp/51173	172.16	tcp/443	🐴 inbound	ter top	
My Views 6/21/12 32.2 Informa 302014 Teardown TCP @ ny-asa 172.16.1.0 top/51168 172.16 top/443 set top All Device Events 2 6/21/12 32.2 Informa 302014 # built TCP @ ny-asa 172.16.1.0 top/51168 172.16 top/443 mound set top 6/21/12 32.2 Informa 302013 # built TCP @ ny-asa 172.16.1.0 top/51168 172.16 top/443 mound set top 6/21/12 32.2 Informa 302013 # built TCP @ ny-asa 172.16.1.10 top/51168 172.16 top/443 mound set top 6/21/12 31 Informa 302013 # built TCP @ ny-asa 172.16.1.10 top/51163 172.16 top/443 mound set top 6/21/12 31 Informa 106015 Denied by S<@ ny-asa		6/21/12 3:2 & Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51170	172.16	tcp/443		10 top	
All Device Events 2 6/21/12 32.2 Informa 302013 # built TCP Invasa 172.16.1.10 ttp/51170 172.16 ttp/443 Imforma 302013 # built TCP Invasa 172.16.1.10 ttp/51188 172.16 ttp/443 Imforma 302013 # built TCP Invasa 172.16.1.10 ttp/51188 172.16 ttp/443 Imforma 302013 # built TCP Invasa 172.16.1.10 ttp/51163 172.16 ttp/443 Imforma 3000 TP Ttp	IPS Error Events	6/21/12 3:2 1 Informa	302013	Buit TCP	S ny-asa	172.16.1.10		tcp/51171	172.16	tcp/443	inbound .	top top	
6/22/12 3:2 informa 302013 # Built TCP Pryses 172.16.1.10 tra/51168 172.16 tra/443 \$ hourd too tra- 6/22/12 3:1 Informa 106015 Dened by S Pryses 172.16.1.10 tra/51163 172.16 tra/443 \$ top/443 \$	My Views	6/21/12 3:2 4 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51168	172.16	tcp/443		10 top	
6/21/12 3:1 Informe 106015 Denied by S S nyasa 172.16.1.10 top/51163 172.16 top/443 BP top 400 AM 500 AM 600 AM 700 AM 900 AM 900 AM 1000 AM 1100 AM 11200 PM 100 PM 200 PM 300 PM	All Device Events 2	6/21/12 3:2 4 Informa	302013	Buit TCP	S ny-asa	172.16.1.10		tcp/51170	172.16	tcp/443	inbound 🖏	top top	
2		6/21/12 3:2 4 Informa	302013	Built TCP	S ny-asa	172.16.1.10		tcp/51168	172.16	tcp/443	inbound	IC top	
2 0 400 AM 500 AM 600 AM 700 AM 800 AM 800 AM 900 AM 1000 AM 1100 AM 1200 PM 100 PM 200 PM 300 PM		6/21/12 3:1 1 Informa	106015	Denied by S	S ny-asa	172.16.1.10		tcp/51163	172.16	tcp/443		top top	
Event Details			AM 6	1,001 10	100 AM		10.00 A	M 11.00	AM 12:00 PM	M 1.00 PM 2.0	0 PM 3)		•
		🖂 Event Details							11				(

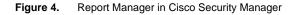
The Event Manager in Cisco Security Manager provides:

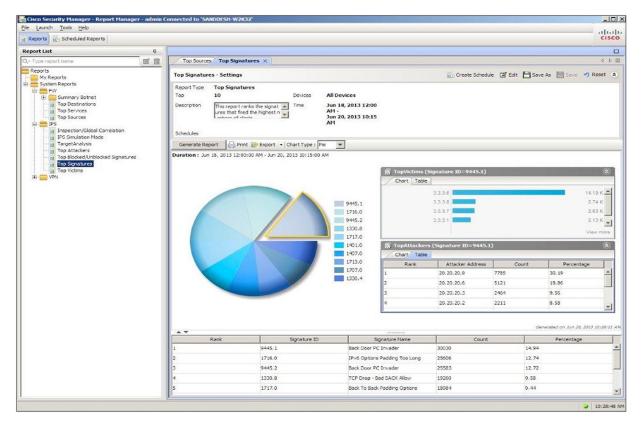
- Support for syslog messages created by Cisco ASA appliances, the Cisco Firewall Services Module (FWSM), and Cisco Catalyst[®] 6500 Series ASA Services Module, as well as Security Device Event Exchange (SDEE) messages from Cisco IPS sensors
- · Real-time and historical event viewing
- · Cross-linkages 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: <u>http://www.cisco.com/go/securitypartners</u>.

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.







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

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.

	0							CISC
A Monitoring								
- Priori	ty Devices	🛃 All Device	s X					4 Þ
Summary								
0			Export +				Last Up	date Time : Jun 12, 2013 3:07:19
Device Name		Receive Time		Health Status 👻	Connection Status 👻	CPU(%)		 Inspection Load(%)
- 🖉 🌮 10.3	77.208.171	Wed Jun 12 15	5:01:00 IST 2013	Critical	Connected	0%	57%8.4(2)	
-0 0 10.1	106.160.53	Wed Jun 12 15	5:01:00 IST 2013	3 Critical	Connected	0%	26%8.4(4)9	
\$ 10.106	5.161.50	Wed Jun 12 15	5:01:00 IST 2013	V Normal	Connected	0%	Not Applicable 8.4(4)	
€ ● 🗇 10.1	106.161.200	Wed Jun 12 15	5:01:00 IST 2013	3 Critical	Connected	0%		
			5:01:00 IST 2013		S Connected	59%	94%7.0(1)E4	84%
-			5:01:00 IST 2013	The second second second	S Connected	68%	94%7.0(1)E4	92%
- H			5:01:00 IST 2013		Connected	2%		0%
				-	A		52 101 101 121	
								•
1 million	Alerts	20			Time Frame: Last 1 h	our ×		Last undated : Jun-12, 15:
Device	Alerts		Value	۲	Time Frame: Last 1 h	our •		Last updated : Jun-12, 15:
Property	e Informatio		Value			our •		Last updated : Jun-12, 15:
Property 21 Device		rd		۲	Time Frame: Last 1 h	our		Last updated : Jun-12, 15: Average : 0%
Property	e Informatio e Report Car					our		
Property C Device Metric Interface Sta	e Informatio e Report Car alus	rd Status		(R) Value		our		
C Device Property Device Metric Interface Sta	e Informatio e Report Car alus ace Status	rd Status Critica	al	¥alue *	CPU Utilization (%)	our		
C Device Property C Device Metric Interface Sta	e Informatio e Report Car alus ace Status	rd Status © Critica ddress S		(R) Value	CPU Utilization (%)	our		Average : 0%
Contraction of the second seco	e Informatio e Report Car atus ace Status IP Ad	rd Status Critica ddress S 1.2	al Status	* Value * Protocol	CPU Utilization (%) 75 - 50 -		• •	Average : 0%
C Device Property Device Metric Interface Sta Interface Sta Interface Sta Interface Sta Interface Sta Interface Sta	e Informatio e Report Car alus ace Status IP Ad 20.1.1	rd Status Scritici ddress S 1.2 d	al Status ✔ up	× Value Protocol v up	CPU Utilization (%) 75 - 50 -	our +	1 14 . 51	Average : 0%
C Device Property Device Metric Interface Str Mame outside inside	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔up ✔up	 A value A value	CPU Utilization (%) 75 - 50 - 25 -	14:3	1 14:51	Average : 0%. 0%
C Device Property Device Metric Interface Sti Interface Name outside inside Test	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔ up ✔ up 3 down	 Alue Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11	14:3	1 14:51	Average : 0%
Device Property Device Metric Interface Sti	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔ up ✔ up 3 down	 Alue Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11	14:3	1	Average : 0%. 0%
Image: Constraint of the second sec	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔ up ✔ up 3 down	 Alue Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 - 50 - 25 - 14:07 14:11 Memory Utilization (% 75 -	14:3	1 14:51	Average : 0%. 0% Average : 57%
Image: Constraint of the second sec	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔ up ✔ up 3 down	 Alue Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (% 75 50	14:3	1 14:51	Average : 0%. 0%
Image: Constraint of the second sec	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔ up ✔ up 3 down	 Alue Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 - 50 - 25 - 14:07 14:11 Memory Utilization (% 75 -	14:3	ı 14:51	Average : 0%. 0% Average : 57%
Image: Constraint of the second sec	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔ up ✔ up 3 down	 Alue Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (% 75 50	14:3	• •	Average : 0%. 0% Average : 57%
Image: Construction of the second s	e Informatio e Report Car atus ace Status IP Ad 20.1.1 2.1.1. 21.23	rd Status Status ddress S 1.2 4 .1 4 3.21.2 1	al Status ✔ up ✔ up 3 down	 Alue Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (% 75 50 25 25	14:3) 14:3	• •	Average : 0%. 0% Average : 57%

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.

Launch Help							0.			cise
Images	2	Install Image	Release Notes				Last updat	ed at :	Sun Jan 29 13	:28:24 PST 2012
n All Images	Imag	es								
Repository Images	0	Image	↑ 💌	Туре	-	Version 👻	Location	-	Size 💌	Description
Bundles 💠 💥 🌣	3	asa701-k8.bin	A	ASA System Software	1	7.0.1.ED	🗞 Cisco.com		4.8 MB	Cisco Adaptive See
Bundles	3	asa702-k8.bin	4	SA System Software	3	7.0.2.ED	Cisco.com		4.8 MB	Cisco Adaptive See
ASA 8.3 Golden Image - Lat	3	asa704-k8.bin	4	SA System Software	1	7.0.4.ED	Cisco.com		5.1 MB	Cisco Adaptive Sec
Devices 🌣	3	asa705-k8.bin	4	SA System Software		7.0.5.ED	Cisco.com		5.2 MB	Cisco Adaptive See
Device Groups	3	asa706-k8.bin	,	ASA System Software		7.0.6.ED	Cisco.com		5.2 MB	Cisco Adaptive See
- 🤭 Department - 🦂 Location	3	asa707-k8.bin	4	SA System Software		7.0.7.ED	Cisco.com		5.2 MB	Cisco Adaptive See
E 🧐 All	3	asa708-12-k8.bin	4	SA System Software		7.0.8 Interim	Cisco.com		5.2 MB	Cisco Adaptive See
	3	asa708-13-k8.bin	4	SA System Software		7.0.8 Interim	Cisco.com		5.2 MB	Cisco Adaptive See
lobs	3	asa708-8-k8.bin	4	SA System Software		7.0.8 Interim	Cisco.com		5.2 MB	Cisco Adaptive See
) Install Jobs	3	asa708-k8.bin	A	SA System Software	1	7.0.8.GD	Cisco.com		5.2 MB	Cisco Adaptive See
	3	asa711-k8.bin	4	SA System Software	1	7.1.1.ED	Cisco.com		6.4 MB	Cisco Adaptive See
		asa712-k8.bin	,	SA System Software		7.1.2.ED	Cisco.com		6.4 MB	Cisco Adaptive Sec

Figure 6.	Software Image Upgrade Wizard in Cisco Security Manager
i igui o oi	Contrare image opgrade imala in close coounty 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	Easily and effectively manages IPS-based configuration and update policies for:
policies	 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.

Support for common VPN deployment scenariosSupports common VPN deployment scenarios with support for Group Encrypted Dynamic Multipoint VPN (DMVPN), and generic routing encapsulation (GRE) IP S IP and hierarchical certificates.Multiple context configurationsSupports policy segmentation and flexibility with security configurations between multiple locations.Remote configurationCentralizes the management of VPNs.Efficiency and Usability FeaturesCan tag changes made in multiple ticketing systems with a single ticket identifier, audit.Global searchCan find all devices, policies, and policy objects in the configuration database tha service.Find usageHelps administrators quickly find usage information about objects by pointing to th policy object, in addition to providing details about all the policies that use the objiAuto-conflict detectionProvides a clear picture about rule conflicts to simplify rule optimization and troub Supports configurations.Integrated event managementHelps enable administrators to monitor status and troubleshoot security information ereses of syslog messages from Cisco ASA appliances and Security Device messages from Cisco IPS sensors• Real-time and historical event views • Cross-linkages to firewall access rules and IPS signatures for quick navigation • 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	Security (IPsec), both with dynamic different branch offices spanning. , making them easily queried for at use a particular IP address or he exact rules that use a particular ect. pleshooting. up deployments and improve on, by providing: e Event Exchange (SDEE)
configurationsmultiple locations.Remote configurationCentralizes the management of VPNs.Efficiency and Usability FeaturesTicketing integrationCan tag changes made in multiple ticketing systems with a single ticket identifier, audit.Global searchCan find all devices, policies, and policy objects in the configuration database tha service.Find usageHelps administrators quickly find usage information about objects by pointing to th policy object, in addition to providing details about all the policies that use the objAuto-conflict detectionProvides a clear picture about rule conflicts to simplify rule optimization and troub compatibility between policy configurations.Integrated event managementHelps enable administrators to monitor status and troubleshoot security information • Receipts of syslog messages from Cisco ASA appliances and Security Device messages from Cisco IPS sensors • Real-time and historical event views • Cross-linkages to firewall access rules and IPS signatures for quick navigation • Prebundled sets of views for firewall, IPS, and VPN monitoring • Customizable views for monitoring select devices or a select time range	making them easily queried for at use a particular IP address or he exact rules that use a particular ect. pleshooting. up deployments and improve on, by providing: e Event Exchange (SDEE)
Efficiency and Usability FeaturesTicketing integrationCan tag changes made in multiple ticketing systems with a single ticket identifier, audit.Global searchCan find all devices, policies, and policy objects in the configuration database that service.Find usageHelps administrators quickly find usage information about objects by pointing to th policy object, in addition to providing details about all the policies that use the objicAuto-conflict detectionProvides a clear picture about rule conflicts to simplify rule optimization and troub Supports configuration of unified IPv4 and IPv6 policies and rules to help speed u compatibilityIntegrated event managementHelps enable administrators to monitor status and troubleshoot security information nessages from Cisco IPS sensors • Real-time and historical event views • Cross-linkages to firewall access rules and IPS signatures for quick navigation • Prebundled sets of views for firewall, IPS, and VPN monitoring • Customizable views for monitoring select devices or a select time range	at use a particular IP address or he exact rules that use a particular ect. oleshooting. up deployments and improve on, by providing: e Event Exchange (SDEE)
Ticketing integrationCan tag changes made in multiple ticketing systems with a single ticket identifier, audit.Global searchCan find all devices, policies, and policy objects in the configuration database that service.Find usageHelps administrators quickly find usage information about objects by pointing to the policy object, in addition to providing details about all the policies that use the object Auto-conflict detectionIntegrated event managementSupports configuration of unified IPv4 and IPv6 policies and rules to help speed of compatibility between policy configurations.Integrated event managementHelps enable administrators to monitor status and troubleshoot security information exclusion of systems of firewall access rules and IPS signatures for quick navigation of Prebundled sets of views for firewall, IPS, and VPN monitoring e Customizable views for monitoring select devices or a select time range	at use a particular IP address or he exact rules that use a particular ect. oleshooting. up deployments and improve on, by providing: e Event Exchange (SDEE)
audit.Global searchCan find all devices, policies, and policy objects in the configuration database that service.Find usageHelps administrators quickly find usage information about objects by pointing to the policy object, in addition to providing details about all the policies that use the object Auto-conflict detectionPrevides a clear picture about rule conflicts to simplify rule optimization and troub lPv4 and IPv6 cross- compatibilitySupports configuration of unified IPv4 and IPv6 policies and rules to help speed u compatibility between policy configurations.Integrated event managementHelps enable administrators to monitor status and troubleshoot security information enessages from Cisco IPS sensors enessages from Cisco IPS sensors enessages for Cisco-Signatures for quick navigation enessages to firewall access rules and IPS signatures for quick navigation enessages for monitoring select devices or a select time range	at use a particular IP address or he exact rules that use a particular ect. oleshooting. up deployments and improve on, by providing: e Event Exchange (SDEE)
service.Find usageHelps administrators quickly find usage information about objects by pointing to the policy object, in addition to providing details about all the policies that use the object and the policies and the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, in addition to providing details about all the policies that use the object and the policy object, and th	he exact rules that use a particular lect. leshooting. up deployments and improve on, by providing: e Event Exchange (SDEE)
Auto-conflict detectionProvides a clear picture about rule conflicts to simplify rule optimization and troubIPv4 and IPv6 cross- compatibilitySupports configuration of unified IPv4 and IPv6 policies and rules to help speed u compatibility between policy configurations.Integrated event managementHelps enable administrators to monitor status and troubleshoot security information ensages from Cisco IPS sensors 	ect. pleshooting. up deployments and improve on, by providing: e Event Exchange (SDEE)
IPv4 and IPv6 cross- compatibility Supports configuration of unified IPv4 and IPv6 policies and rules to help speed u Integrated event management Helps enable administrators to monitor status and troubleshoot security information Receipts of syslog messages from Cisco ASA appliances and Security Device messages from Cisco IPS sensors Real-time and historical event views Cross-linkages to firewall access rules and IPS signatures for quick navigation Prebundled sets of views for firewall, IPS, and VPN monitoring Customizable views for monitoring select devices or a select time range Supports configuration	up deployments and improve on, by providing: e Event Exchange (SDEE)
compatibility compatibility between policy configurations. Integrated event management Helps enable administrators to monitor status and troubleshoot security information • Receipts of syslog messages from Cisco ASA appliances and Security Device messages from Cisco IPS sensors • Real-time and historical event views • Cross-linkages to firewall access rules and IPS signatures for quick navigation • Prebundled sets of views for firewall, IPS, and VPN monitoring • Customizable views for monitoring select devices or a select time range	on, by providing: e Event Exchange (SDEE)
management • Receipts of syslog messages from Cisco ASA appliances and Security Device messages from Cisco IPS sensors • Real-time and historical event views • Cross-linkages to firewall access rules and IPS signatures for quick navigation • Prebundled sets of views for firewall, IPS, and VPN monitoring • Customizable views for monitoring select devices or a select time range	e Event Exchange (SDEE)
 Administrative options to turn event collection on or off for select security devi Launch of the Cisco Prime[™] Security Manager when an ASA CX deployment 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 • Viewed as charts and grids • Exported as PDF or Excel files • Scheduled for delivery by email • Scanned for more detail	be:
Bulk operations Reduces administrative overhead in networks that have a large number of device • 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 deploye 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 all devices in a group as a single device.	ction or location, and then manage
Policy Object Manager Defines objects such as network addresses, services, device settings, time range then uses them any number of times to avoid manual entry of values.	es, or VPN parameters once and
Other Capabilities	
Third-party device support Supports "unmanaged" endpoints and third-party devices.	
Security services Manages integrated security services, including quality of service (QoS) for VPN, Admission Control (NAC).	routing, and Cisco Network
Multiple application views Provides multiple views into the application to support different use cases and ex	perience levels.
Flexible deployment or a scheduled base options	sis.
Rollback Can roll back deployments to a previous configuration if required.	
Role-based access Defines and enforces up to five administrator roles; additional roles are available Access Control Server (ACS).	with the optional Cisco Secure
Workflow Can assign specific tasks to each administrator during the deployment of a policy tracking.	v, with formal change control and

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, 37	50 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: <u>http://www.cisco.com/go/csmanager</u>.

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: <u>http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html</u>.

- 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: <u>http://www.cisco.com/security</u>.
- **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 <u>http://www.cisco.com/en/US/products/ps6498/index.html</u> or contact your account manager or a Cisco Authorized Technology Provider. You may also send an email to <u>ask-csmanager@cisco.com</u>.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA