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.

uluulu Cisco Security Manager				User: rakesh Server: 10.142.52
cisco	🚱 Configuration	Manager 🚑 Event Viewer	👹 Health and Performance Monitor 🝓 I	nage Manager 🛛 欇 Report Man
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 • 🔍 Type to Search	Signatures	Last 24 Hours 👻	IP Address	Last 24 Hours
Na Device Down 0	Back Door PC Invader (9445.1)	72.88 K	malware.com (192.20.20.20)	501.92
🔤 Interface Down 3	IPv6 Options Padding Too Long (1716.0)	61.7 K	malware.com (172.30.30.30)	501.92
W Overall Device Health 6	Back Door PC Invader (9445.2)	61.65 K		
High CPU Utilization 0	TCP Drop - Bad SACK Allow (1330.8)	50 K		
High Memory Utilization	Invalid IPv6 Header Flow Label Field (1707.0)	47.77.K		
A IPS - High Inspection Load 2		View more		
E 🔔 IPS - High Missed Packets	Top Attackers Last	updated on Jun-11, 02:24 PM	Top Sources	Last updated on Jun-11, 02:24 P
A IPS - Bypass Mode 2				Last updated on Jun-11, U2:24 P
2 (F 3 - Dypass mode 2	Attackers	Last 24 Hours 👻	Sources	
	20.20.20.3	89.06 K	192.20.20.20	752.9
	20.20.20.1	69.62 K		
	10.10.10.1	59.38 K		
	10.10.10.100	57.9 K 55.66 K		
	20.20.20.2			
		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		
	22.2.1	56.42 K		
	3.3.3.2	55.66 K		
		View more		
Top Infected Hosts Last updated on Jun-11, 02:24 P			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		
		8 Expired		

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).

Polcy Assgned To: 3 Devices Inherits From: none Polcy Assgned: Global FW-Polcy Assgned To: 3 Devices Inherits From: none Polcy Assgned: Sabal FW-Polcy Mail Inherits From: none Polcy Assgned: Sabal FW-Polcy Mail Service Inherits From: none Polcy Assgned: Sabal FW-Polcy Mail Service Inherits From: none No. Permit Source User Destination Service Inherits From: none No. Permit Source User Destination Service Inherits From: none No. Permit Source User Destination Service Inherits From: none No. Permit Source User Destination Service Inherits From: none No. Permit Source User Destination Service Inherits From: none No. Permit Source User Destination Service P Global 1 Ø # any THREATDLASS(Writg DataCenter-1 P P Global 5 <td< th=""><th>Device Map Device Po</th><th></th><th></th><th></th><th></th><th></th><th>1 9</th><th>Search All C</th><th>Cleategories</th></td<>	Device Map Device Po						1 9	Search All C	Cleategories
Location Al Al Al Cosas Al Al Cosas <pc< th=""><th></th><th>Policy As</th><th>signed:</th><th>Global F</th><th></th><th></th><th>L</th><th>Inherits From: none</th><th></th></pc<>		Policy As	signed:	Global F			L	Inherits From: none	
All No. Permit Source User Destination Service Interface Image: Service		+ Filte	er: (no	one)					
Image: Second PUP Poincy - Mandatory (25 Rules) Image: Second Pup Poince		No		Permit	Source	User	Destination	Service	Interface
Image: Second State Sta		E	ST Glo	bal FW Po	licy - Mandatory (23 Rules)				-
2 S Bany THREATDLABS\Wikitg DataCenter-2 FIP Coloration Sources 3 S Bany THREATDLABS\Wikitg DataCenter-3 FIP Coloration Aldices 3 S Bany THREATDLABS\Wikitg Coloration FIP Coloration Aldices 4 S Bany THREATDLABS\Wikitg Coloration FIP Coloration AAA Rules 5 S Bany THREATDLABS\Wikitg Coloration FIP Coloration AAA Rules 6 Bany THREATDLABS\Wikitg DataCenter-1 FIP Coloration AAA Rules Access Rules 6 Bany THREATDLABS\Wikitg DataCenter-2 FIP Coloration IPv6 Access Rules 6 Bany THREATDLABS\Wikitg DataCenter-3 FIP Coloration IPv6 Access Rules 6 Bany THREATDLABS\Wikitg DataCenter-1 FIP Coloration IPv6 Access Rules 10 Bany THREATDLABS\Wikitg DataCenter-3 FIP Coloration IPv6 Biolobal 9 <td></td> <td></td> <td>1</td> <td>0</td> <td>any any</td> <td>THREATDLABS\\Mktg</td> <td>DataCenter-1</td> <td>D IP</td> <td>() Global</td>			1	0	any any	THREATDLABS\\Mktg	DataCenter-1	D IP	() Global
3 3			2	0	🍰 any	THREATDLABS\Wktg	DataCenter-2	D IP	Global
4 O aff any THREATDLABS\Wikitg CSM-Server P fig Gobal incices 5 O aff any THREATDLABS\Wikitg CSM-Server P fig Gobal incices 6 O aff any THREATDLABS\Wikitg DataCenter-1 P fig Gobal Firewall 6 O aff any THREATDLABS\\Fr g DataCenter-2 P P fig Gobal 7 O aff any THREATDLABS\\Fr g DataCenter-3 P P fig Gobal 8 O aff any THREATDLABS\\Fr g DataCenter-3 P P fig Gobal 9 O aff any THREATDLABS\\Fr g DataCenter-3 P P fig Gobal 9 O aff any THREATDLABS\\Fr g DataCenter-1 P fig Gobal 9 O aff any THREATDLABS\\Fr g DataCenter-3 P P fig Gobal 10 O aff any THREATDLABS\\Fr g DataCenter-3 P P fig Gobal 11 O <			3	0	👼 any	THREATDLABS\Wktg	DataCenter-3	D IP	Global
Indees 6 O ge any THREATDLABS\\Br ge DataCenter-2 prove ge Global Frewall AAA Rules 7 O ge any THREATDLABS\\Br ge DataCenter-3 prove ge Global AAA Rules Aada Rules 9 O ge any THREATDLABS\\Br ge DataCenter-3 prove ge Global 9 O ge any THREATDLABS\\Br ge CSM-Server prove prove ge Global 9 O ge any THREATDLABS\\Br ge CSM-Server prove prove ge Global 9 O ge any THREATDLABS\\Eng ge DataCenter-1 prove ge Global 9 O ge any THREATDLABS\\Eng ge DataCenter-2 prove ge Global 11 O ge any THREATDLABS\\Eng ge DataCenter-3 prove ge Global 12 O ge any THREATDLABS\\Eng ge DataCenter-3 prove ge Global 12 O ge any THREATDLABS\\Eng ge DataCenter-3 prove ge Global 13 O ge any THREATDLABS\\Eng ge D	Sil@sf-asa		4	0	any any	THREATDLABS\Wktg	CSM-Server	P IP	(Bobal
Frewall 6 6 9 </td <td></td> <td></td> <td>5</td> <td>0</td> <td>any any</td> <td>THREATDLABS\\Br</td> <td>DataCenter-1</td> <td>P IP</td> <td>() Global</td>			5	0	any any	THREATDLABS\\Br	DataCenter-1	P IP	() Global
AAA Rules 8 S B any THREATDLABS\\Engg CSM-Server D IP C Global Pro6 Access Rules 9 S B any THREATDLABS\\Engg DataCenter-1 D IP C Global Inspection Rules 10 S B any THREATDLABS\\Engg DataCenter-2 D IP C Global Inspection Rules 10 S B any THREATDLABS\\Engg DataCenter-2 D IP C Global Inspection Rules 10 S B any THREATDLABS\\Engg DataCenter-3 D IP C Global Inspection Rules 11 S B any THREATDLABS\\Engg DataCenter-3 D IP C Global NAT II B any THREATDLABS\\Engg DataCenter-3 D IP C Global NAT II B any THREATDLABS\\Engg DataCenter-3 D IP C Global Interfaces II III III IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	licies		6	0	any any	THREATDLABS\\Br	DataCenter-2	P IP	Global E
Access Rules 9 <t< td=""><td>Firewall</td><td></td><td>7</td><td>0</td><td>any any</td><td>THREATDLABS\\Br</td><td>DataCenter-3</td><td>P IP</td><td>(B) Global</td></t<>	Firewall		7	0	any any	THREATDLABS\\Br	DataCenter-3	P IP	(B) Global
IPV6 Access Rules 9 Important Stress 9 Important Stress			8	0	any any	THREATDLABS\\Br	CSM-Server	P IP	(Global
Inspection Rules 10 Image: Section Structure Rules 11 Image: Section Structure Rules 11 Image: Section Structure Rules 11 Image: Section Structure Rules 12 Image: Section Structure Rules 13 Image: Section Structure Rules 14 Image: Section Structure Rules 14 Image: Section Structure Rules 15 Image: Section Structure Rules 16 Section Structure Rules 17 Image: Section Structure Rules 17 <td></td> <td></td> <td>9</td> <td>0</td> <td>any any</td> <td>THREATDLABS\\Engg</td> <td>DataCenter-1</td> <td>P IP</td> <td>(Biobal</td>			9	0	any any	THREATDLABS\\Engg	DataCenter-1	P IP	(Biobal
→ Settings 11 ● age of y Interfaces (prog age objective of age of y) 12 ● age of y Interfaces (prog age objective of age of y) 10 (a) Global 12 ● age of y THREATDLABS\\Engg age objective of y 10 (a) Global 13 ● age of y ··· no user ·· 7.7.7.7 (b) IP (a) Global 13 ● age of y ··· no user ·· 7.7.7.7 (b) IP (a) Global 13 ● age of y ··· no user ·· 7.7.7.7 (b) IP (b) Global 14 ✓ age of y THREATDLABS\\Engg age objective of y (b) IP (b) Global [] Identity Options (c) If ✓ age of y (c) Ithreat TDLABS\\Engg age objective of y (c) IP (c) Global Platform 12 ✓ age of plateoring Net THREATDLABS\\Engg age objective of y (c) IP (c) Global			10	0	any	THREATDLABS	DataCenter-2	P IP	(Bobal
Web Filter Rules 12 Image: Second Secon			11	0	any any	THREATDLABS\\Engg	DataCenter-3	P IP	Global
NAT 13 Image: Bary no user 7.7.7 Image: Pipe Biological Biologica			12	0	any any	THREATDLABS\\Engg	CSM-Server	PI 😥	() Global
Remote Access VPN Image: Strategy and the str	-		13	0	any any	no user	7.7.7.7	PI 🙀	Global
Remote Access VPN Image: Second	Site to Site VPN	0		~	any	THREATDLABS\\Sa	8.8.8.8	PI 😪	Global
Differences Identity Options		-		V		THREATDLABS\\Engg	DataCenter-1	PI P	
Platform 17 🗸 🛞 Engineering Net THREATDLABS\\Engg AB DataCenter-3 🖨 IP 🖀 Global	2	-		×	Engineering_Net	THREATDLABS	DataCenter-2	PI 😥	Global
Encodings	Platform FlexConfigs	~	17	~	R Engineering Net	THREATDLABS\\Enoo	DataCenter-3	PI	(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 Views All Device Events All Device Events Search within results: C- Type here to search C list 12 hour + All Events (Default) + Sourch +	rs t	Event Monitoring												
Image: Construction	iew 🛒 Edit 🏢 Delete	All Device Events	Firewall T	raffic Events >	K E Frewa	I Denied Events 22	NAT Events					4	1 1	
Second Traffe Second Frenced Traffe Second AAA Events Second Traffe Second Frenced Devide Second AAA Events Second Traffe Second Frenced Devide Second AAA Events Second Traffe Second Frenced Devide Second Second Provide Second Provide Second Second Provide Second Provid		😵 View Settings 炎												
AAA Events Receive Tim. Seventy Y Ev Event Name Device Sourc. Court. <		Search within results: Q Typ	pe here to sear	rch	🐼 last 1	2 hour · All Events (De	efault) 🔹 🔛 S	ave - 🕨 Si	tart 🔳 Stop 👔	Clear			3,	
6/2/11/2 32: 4 Informa 302114 Teardown TCP @ ny-sea 172:15 100 100/51175 172:15 100/443 100 cm 8 bbshe Events 6/2/1/2 32: 4 Informa 30214 Teardown TCP @ ny-sea 172:1510 tcp/51175 172:15 tcp/443 100 cm 9 PSe VM Events 6/2/1/2 32: 4 Informa 30213 #Buit TCP @ ny-sea 172:1510 tcp/51175 172:15 tcp/443 100 cm 100 cm 9 PSe VM Events 6/2/1/2 32: 4 Informa 30213 #Buit TCP @ ny-sea 172:1510 tcp/51175 172:15 tcp/443 100 cm 100 cm <th>Mart .</th> <th>Receive Ti Severity -</th> <th>Y Ev •</th> <th>Event Name</th> <th>Device +</th> <th>Source -</th> <th>Sourc •</th> <th>Sourc •</th> <th>Destin •</th> <th>Destin Desti</th> <th>n • Direction •</th> <th>Protocol</th> <th></th>	Mart .	Receive Ti Severity -	Y Ev •	Event Name	Device +	Source -	Sourc •	Sourc •	Destin •	Destin Desti	n • Direction •	Protocol		
6/2/1/2 32 6 forma 30014 Tendown TCP © ny-asa 172.1610 top/51.75 172.16 top/443 ten top/443		6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51178	172.16	tcp/44	3	top top	-	
6 S2/12 3:2 a Informa 302014 Teardown TCP @ ny-asa 172.1610 tcp/51173 172.16 tcp/443 tsp rbord tsp tcp 7 Blower Events 6/21/12 3:2 a Informa 302014 Teardown TCP @ ny-asa 172.1610 tcp/51173 172.16 tcp/443 tsp rbord tsp tcp 7 Blower Events 6/21/12 3:2 a Informa 302014 Teardown TCP @ ny-asa 172.1610 tcp/51173 172.16 tcp/443 tsp rbord tsp tcp 7 D5 Status Events 6/21/12 3:2 a Informa 302014 Teardown TCP @ ny-asa 172.1610 tcp/51173 172.16 tcp/443 tsp rbord tsp tcp 7 D5 Status Events 6/21/12 3:2 a Informa 302014 Teardown TCP @ ny-asa 172.1610 tcp/51173 172.16 tcp/443 tsp rbord tsp tcp 8/21/12 3:2 a Informa 302014 Teardown TCP @ ny-asa 172.1610 tcp/51173 172.16 tcp/443 tsp rbord tsp tcp 8/21/12 3:2 a Informa 302013 #B buit TCP @ ny-asa 172.1610 tcp/51168 172.1		6/21/12 3:2 4 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51175	172.16	tcp/44	3	top		
Fallower Events 000141 # 21.0 1000401 4000401 1000401 1000401 1000403 <		6/21/12 3:2 4 Informa	302013	Built TCP	S ny-asa	172.16.1.10		tcp/51178	172.16	tcp/44	3 🐴 inbound	top top		
All DP Strents 0/4/14 25 a Informa 200013 # Built TCP % ny-ses 172.1610 tup/91.73 172.16 tup/943 # inbornd tes top 6/21/12 32 a Informa 200013 # Built TCP % ny-ses 172.1610 tup/91.73 172.16 tup/943 # inbornd tes top 6/21/12 32 a Informa 200141 Texadown TCP % ny-ses 172.1610 tup/91.73 172.16 tup/943 # inbornd tes top 6/21/12 32 a Informa 200141 Texadown TCP % ny-ses 172.1610 tup/91.73 172.16 tup/943 # inbornd tes top f/21/12 32 a Informa 200131 # Built TCP % ny-ses 172.1610 tup/91.77 172.16 tup/943 # inbornd tes top f/21/12 32 a Informa 200131 # Built TCP % ny-ses 172.1610 tup/91.77 172.16 tup/9433 # inbornd tes top f/21/12 32 a Informa 200131 # Built TCP % ny-ses 172.1610 tup/911.70 172.16		6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51173	172.16	tcp/44	3	tcp		
Open Norty Alerts		6/21/12 3:2 1 Informa	302013	Built TCP	S ny-asa	172.16.1.10		tcp/51175	172.16	tcp/44	3 🐴 inbound	top		
Operator		6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51171	172.16	tcp/44	3	top top		
bp:Status Events 6/2/1/2 3:2 A Informa 302013 AB buit TCP Pry-sea 172:16 tcp/413 Ise top Al Device Events 2 6/2/1/2 3:2 A Informa 302013 AB buit TCP Pry-sea 172:1610 tcp/51:70 172:16 tcp/443 Ise top Al Device Events 2 A Informa 302013 AB buit TCP Pry-sea 172:1610 tcp/51:70 172:16 tcp/443 Ise top 6/2/1/2 3:2 A Informa 302013 AB buit TCP Pry-sea 172:1610 tcp/51:70 172:16 tcp/443 Ise top 6/2/1/2 3:2 A Informa 302013 AB buit TCP Pry-sea 172:1610 tcp/51:70 172:16 tcp/443 Ise top 6/2/1/2 3:2 A Informa 302013 AB buit TCP Pry-sea 172:1610 tcp/51:163 172:16 tcp/443 Ise top 6/2/1/2 3:2 A Informa 302013 AB buit TCP Pry-sea 172:1610 tcp/51:163 172:16 tcp/51:163		6/21/12 3:2 4 Informa	302013	H Buit TCP	S ny-asa	172.16.1.10		tcp/51173	172.16	tcp/44	3 🐴 inbound	tep tep		
My Weins 6/21/12 3:2 Informa 302014 Teardown TCP Physics 172.1610 tcp/51163 172.16 tcp/443 Bit hourd		6/21/12 3:2 1 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51170	172.16	tcp/44	3	10 top		
Al Device Events 2 6/21/12 3:2 a Informa 302013 #Built TCP @ ny-asa 6/21/12 3:2 a Informa 302013 #Built TCP @ ny-asa 172.1610 top/51163 172.16 top/443 Built TCP @ ny-asa 172.1610 top/51163 172.16 top/443 Built TCP #B top 6/21/12 3:1 a Informa 106015 Denied by S @ ny-asa 172.1610 top/51163 172.16 top/443 Built TCP @ ny-asa 172.1610 top/51163 172.16 top/443 Built TCP @ ny-asa 172.16 10 top/51163 172.16 top/443 Built TCP @ ny-asa 172.16 top/143 Built TCP @ ny-asa 172.16 top/443 Built TCP @ ny-asa 172.16 top/143 Built TCP @ ny-asa 172.16 top/443 Built TCP @ ny-asa 172.16 top/143 Built TC	IPS Error Events	6/21/12 3:2 1 Informa	302013	Built TCP	S ny-asa	172.16.1.10		tcp/51171	172.16	tcp/44	3 🐴 inbound	top top		
6/21/12 3:2 toforms 00013 6 Built TCP or ny-asa 12:16:1:10 top/51163 172:16 top/443 5 indoced are top for to		6/21/12 3:2 4 Informa	302014	Teardown TCP	S ny-asa	172.16.1.10		tcp/51168	172.16	tcp/44	3	10 top		
6/21/12 3:1 Informa 106015 Denied by S 🔅 ny-asa 172.16.1.10 top/51163 172.16 top/443 🕸 top	— All Device Events 2	6/21/12 3:2 1 Informa	302013	Buit TCP	S ny-asa	172.16.1.10		tcp/51170	172.16	tcp/44	3 🐴 inbound	tcp		
C C C C C C C C C C C C C C C C C C C		6/21/12 3:2 1 Informa	302013	Built TCP	S ny-asa	172.16.1.10		tcp/51168	172.16	tcp/44	3. 🐴 inbound	10 top		
2			106015	Denied by S		172.16.1.10		tcp/51163	172.16	tcp/44	3	10 top		
S Event Details			DAM 6	1 III 1	100 AM		M 10.00 A	M 11.00	AM 12:00 I	PM 1:00 PM	2.00 PM 3		•	
		😑 Event Details			1				1				(

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
P Monitoring	-							
Priorit	ty Devices	🛃 All Devi	ces ×					4 Þ
Summary								
Q			🔥 Export 👻				Last Upd	late Time : Jun 12, 2013 3:07:19
Device Name		Receive Tin		Health Status 👻	Connection Status 👻	CPU(%)		Inspection Load(%)
	77.208.171	Wed Jun 12	15:01:00 IST 2013	Critical	Connected	0%		
-0 0 10.1	106.160.53	Wed Jun 12	15:01:00 IST 2013	3 Critical	Connected	0%	26%8.4(4)9	
S 10.106	.161.50	Wed Jun 12	15:01:00 IST 2013	🖌 Normal	Connected	0%	Not Applicable 8.4(4)	
• • • 10.1	106.161.200	Wed Jun 12	15:01:00 IST 2013	3 Critical	Connected	0%		
			15:01:00 IST 2013		Connected	59%	94%7.0(1)E4	84%
-			15:01:00 IST 2013		Connected	68%		92%
-			15:01:00 IST 2013		Connected	2%		0%
- 0,- 11.				-				
								•
Tevice	Informatio	on		۲	Time Frame: Last 1 ho	our		Last updated : Jun-12, 15:0
Property			Value		Time Frame: Last 1 ho	our ·		Last updated : Jun-12, 15:0
Property	e Informatio e Report Car	rd		۲	Time Frame: Last 1 ho CPU Utilization (%)	our v		
Property Control Property Metric	e Report Car	rd Status				our		Last updated : Jun-12, 15.0 Average : 0%
Property	e Report Car	rd		۲		our •		
Property C Device Metric Interface Sta	e Report Car	rd Status		۲	CPU Utilization (%)	our		Average : 0%
Property C Device Metric Interface Sta Mame	e Report Car alus ace Status IP Ad	rd Status Status Crit	tical Status	 Xalue Protocol 	CPU Utilization (%) 75 - 50 -	our		
Property C Device Metric Interface Sta Mame outside	e Report Car alus ace Status IP Ad 20.1.	rd Status Status crit ddress 1.2	s ical Status ✔ up	 Xalue Protocol y up 	CPU Utilization (%)	our •		Average : 0%
Property Construction Metric Interface Sta Interface Sta Interface Name outside inside	e Report Car atus ace Status IP Ad 20.1. 2.1.1	rd Status Status crit ddress .1.2 .1	status ✔ up ✔ up	 A Value A Value A Protocol A up A up 	CPU Utilization (%) 75 - 50 - 25 -		11 1451	Average : 0%
Property Device Metric Interface Sta Interface Sta Interface Name outside inside Test	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11	14:3	11 14:51	Average : 0%
Property Device Metric Interface Sta Marne outside inside	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status crit ddress .1.2 .1	status ✔ up ✔ up	 A Value A Value A Protocol A up A up 	CPU Utilization (%) 75 - 50 - 25 -	14:3	14 ¹ 51	Average : 0%
Property Device Metric Interface Sta Interface	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11	14:3	il 14:51	Average : 0%
Property Device Metric Interface Sta Interface Sta Name outside inside Test	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11	14:3	91 1 4:51	Average : 0%
Property Device Metric Interface Sta Interface	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (%)	14:3	11 14:51	Average : 0%
Property Device Metric Interface Sta Interface	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (%) 75 50	14:3	14:51 °	Average : 0%
Property Device Metric Interface Sta Interface Sta Interface Name outside inside Test	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (%) 75	14:3	14:51	Average : 0%
Property Device Metric Interface Sla Interface	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (%) 75 50	14:3		Average : 0%
Property Device Metric Interface Sta Interface Sta Interface Name outside inside Test	e Report Car atus ace Status IP Ad 20.1. 2.1.1. 21.23	rd Status Status Crit ddress .1.2 .1 .1 3.21.2	status ✓ up ✓ up 3 down	 A Value A Protocol ✓ up ✓ up ✓ down 	CPU Utilization (%) 75 50 25 14:07 14:11 Memory Utilization (%) 75 50 25)) 14:3		Average : 0%

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.

E Launch Help							Q	5		ciso
Images	3	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	4	ASA System Software		7.0.1.ED	Cisco.com		4.8 MB	Cisco Adaptive Sec
Bundles	3	asa702-k8.bin	4	SA System Software		7.0.2.ED	Cisco.com		4.8 MB	Cisco Adaptive Sec
ASA 8.3 Golden Image - Lat	3	asa704-k8.bin	1	SA System Software		7.0.4.ED	Cisco.com		5.1 MB	Cisco Adaptive Sec
Devices 🌣	3	asa705-k8.bin	1	SA System Software		7.0.5.ED	Cisco.com		5.2 MB	Cisco Adaptive Sec
Device Groups	3	asa706-k8.bin	,	SA System Software		7.0.6.ED	Cisco.com		5.2 MB	Cisco Adaptive Sec
- 2 Department - 2 Location	3	asa707-k8.bin	1	SA System Software		7.0.7.ED	Cisco.com		5.2 MB	Cisco Adaptive Sec
∃ 🧿 All - 🔗 ny-asa	3	asa708-12-k8.bin	1	SA System Software		7.0.8 Interim	Cisco.com		5.2 MB	Cisco Adaptive Sec
ny-asa so sf-asa		asa708-13-k8.bin	4	SA System Software		7.0.8 Interim	Cisco.com		5.2 MB	Cisco Adaptive Sec
Jobs	3	asa708-8-k8.bin	1	SA System Software		7.0.8 Interim	Cisco.com		5.2 MB	Cisco Adaptive Sec
🔅 Install Jobs	8	asa708-k8.bin	4	SA System Software		7.0.8.GD	Cisco.com		5.2 MB	Cisco Adaptive Sec
	3	asa711-k8.bin	4	SA System Software		7.1.1.ED	Cisco.com		6.4 MB	Cisco Adaptive Sec
	3	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
riguic v.	Contrare intage opgrade	VIZulu III 01000	occurry 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.

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
Zone-based policies	Sets zone-based firewall policies on supported device platforms if desired.

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

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

Feature	Benefit	
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 Cisc	co Security Manager
----------	---------------------------	-------------------	---------------------

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

Ordering Information

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

The latest version of Cisco Security Manager that can be ordered is version 4.5

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