cisco.

Cisco Adaptive Security Device Manager Version 5.2F for Cisco Firewall Services Module Software Version 3.2

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring through an intuitive, easy-to-use Web-based management interface. Bundled with the Cisco Firewall Services Module (FWSM), Cisco ASDM accelerates security deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the Cisco FWSM. The secure, Web-based design of Cisco ASDM enables anytime, anywhere access to Cisco FWSMs located in any part of the network. Based on Cisco ASDM Version 5.2 for Cisco ASA 5500 Series and Cisco PIX security appliances running Cisco PIX[®] Software Version 7.2, Cisco ASDM Version 5.2F enables administrators to use their knowledge to deploy the market-leading suite of Cisco security appliances and services modules.

Integrated Management Solution Provides Flexible Access Options

Cisco Adaptive Security Device Manager (ASDM) can be accessed directly with an Internet browser from any Java plug-in enabled computer or from a Microsoft Windows PC with Cisco ASDM Launcher installed, providing security administrators with rapid and secure access to their Cisco Firewall Services Module (FWSM). The Cisco ASDM Launcher can be downloaded directly from the FWSM and installed on a management computer. This application accelerates the startup of Cisco ASDM, providing increased efficiency in managing security appliances. By running separate instances of the Cisco ASDM launcher application, administrators can connect to multiple FWSMs from the convenience of a single management workstation business.

Startup Wizard Accelerates Security Deployment

Cisco ASDM features a startup wizard that helps accelerate the FWSM deployment process. A series of simple step-by-step configuration panels help administrators get their appliances operating quickly and create a robust configuration that allows traffic to flow securely through their networks. The startup wizard provides the ability to configure optional features such as Dynamic Host Control Protocol (DHCP) server settings, Network Address Translation (NAT), and administrative access. In Multiple Contexts Mode, the startup wizard can also be used for initial setup of newly created contexts.

Dashboard Supplies Administrators with Vital Real-Time System Status Information

Cisco ASDM 5.0F includes a dynamic dashboard that provides a complete system overview and device health statistics at a glance (Figure 1). It can automatically detect the Cisco FWSM being configured; for each, it will display the software version, license information, and important statistics. In complex network environments, it presents administrators with real-time status indicators and provides a launching point to powerful analysis tools and advanced monitoring capabilities—including a real-time syslog viewer with pattern-matching capabilities to filter syslogs based on network addresses, port numbers, host names, and more. This release introduces a powerful search engine that helps administrators locate where specific features can be configured, and provides convenient point-and-click access to the search results.





Robust Security Policy Management Lowers Operational Costs

Cisco ASDM features powerful management services that simplify security policy definition and ongoing policy maintenance by giving security administrators the ability to create reusable network and service object groups and inspection policy maps that can be referenced by multiple security policies. ASDM v5.2F adds complete management support for network, service, protocol, and Internet Control Message Protocol (ICMP)-type object groups to ease configuration. It also supports the wide range of access control features offered by Cisco FWSM Software Version 3.1 and 3.2, such as user-, group-, and time-based access control lists (ACLs), and inbound/outbound ACLs. Cisco ASDM also supports the new powerful and highly flexible Modular Policy Framework, which allows administrators to identify a network flow or a traffic class based on different conditions, and then apply a set of customizable inspection services and connection services to each flow or traffic class. These advanced access control and application inspection capabilities, coupled with easy-to-use ongoing policy management services, help to ensure a robust and dynamic security profile for businesses of all sizes.

Cisco ASDM v5.2F features an all-new integrated policy table that allows administrators to view their complete security policy from the convenience of a single animated panel. Simply clicking on a listed policy allows the editing of all parameters associated with it, thereby simplifying configuration changes and updates. A new object group selector sidebar enables the inline editing of all network and service object groups so they can be rapidly referenced and modified in real time (Figure 2). It also provides a new Rule Query option to allow administrators to quickly filter the various network elements nad object groups of interest for focused monitoring and troubleshooting security policies that employ them.





Business-Class Security Services Enforce Secure, Role-Based Administrative Access

Cisco ASDM Version 5.0F integrates an array of robust security services to prevent unauthorized administrative access to a device. It supports a wide range of methods for authenticating administrators, including a local authentication database on a Cisco FWSM, or via a RADIUS/TACACS server. All communications between Cisco ASDM (running on an administrator's computer) and the security appliance are encrypted using Secure Sockets Layer (SSL) with either 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES) algorithm. Cisco ASDM supports up to 16 levels of customizable administrative access, granting administrators and operations personnel the appropriate level of permissions for every Cisco security appliance they manage (for example, monitor-only, read-only access to the configuration).

Comprehensive Management Services Complement Advanced Application Inspection

Cisco FWSM Software Version 3.1and Version 3.2 includes more than 30 dedicated inspection engines for a range of modern applications driven by protocols such as HTTP (Figure 3), FTP, General Packet Radio Service (GPRS) Tunneling Protocol (GTP), Sun Remote Procedure Call (SunRPC), H.323, and Session Initiation Protocol (SIP). Cisco ASDM enables point-and-click capabilities conditioned by intelligent application defaults to quickly establish robust security profiles that protect mission-critical applications and resources from misuse and tunneling attacks.

It enforces flow-based control in defining inspection services and gives administrators enterpriseclass tools to exercise microscopic control over applications.



Figure 3. Advanced HTTP Inspection Services Configuration

Intelligent User Interface Simplifies Integration Into Complex Network Environments

Cisco ASDM provides easy and convenient access to managing the rich network integration features found in the Cisco FWSM. Virtualization allows the creation of multiple security contexts (virtual firewalls) within a single security appliance, with each context having its own set of security policies, logical interfaces, and administrative domain. Cisco ASDM uses an intelligent virtualization management system to provide unrestricted access for central system administrators who desire complete visibility into all virtual firewalls and features on the system. Individual context users get the same interface as Cisco ASDM, as well as the same rich management and monitoring capabilities. However, configuration and feature access are restricted only to the assigned context, and as specified by the central system administrators. Individual context users can build upon the administrator-created security policies to create a customized configuration for their virtual firewalls using Cisco ASDM.

Cisco ASDM gives administrators complete control over multicast routing protocols such as Protocol Independent Multicast (PIM) (Figure 4), Open Shortest Path First (OSPF) dynamic routing (Figure 5), and IEEE 802.1q-based VLAN interface mechanisms. For novice users, it combines intelligent defaults and detailed online help to simplify configuration of these networking services. Advanced users can take full advantage of the depth of feature support to integrate Cisco FWSM into complex routing and switching environments.

Figure 4. Advanced PIM-SPARSE Multicast Configuration

CT AND ADDRESS OF			
Come Car Come Car	Greifigan Proteini Subgereiteni Milleani (1995 par ereiteni. Ibberteani 1991 basileti Dit Proteini Ibbernali barnati barnali Robet ibbereiti Barrati Barrati ibbereiti	<u> </u>	
ating Alignets D	E	Edit PIM Protocol	
2-9 earton	43	Interface:	Imgmt IF Enable FIM
		DR Priority:	1
<u>د ا</u>	Anter Tool	Helio Interval:	30 seconds
		Join-Prune Interval:	60 seconds

Figure 5. Advanced OSPF Configuration

+ ☆ ▼ (6) (2) / 2	g v DOPT – Tekto	
+	18 S.R. G.	
are the second s	Endo of had one OPP Process Balance and define a sea and one smitheds. Interest instrume years missioning Trade Searchisterian Measure / Searchitter and the cartain for and a file deals. Normalies at OPP 1 the checkson. OPP Process 1 OPP Process 1 (************************************	nosm, Gude 11 Edit OSIP Process Advanced Properties
ecto	ogencos p ji <u>Lavence 1</u>	ps for USIP Process Advanced Properties
	OUP Process 2 The spin the OPP Process COPP (1) and 20	OSPF Process: E Pouter ID:
		Larver LSA MOSP (suppress the sending of systog messages when router receiver a LSA MOSP periodent) (533)
	+	-Adaptency Changes
		Enable this for the Firewall to send a syslog message when an OSPF neighbor goes up/down. Enable this for the Firewall to send a syslog for each state change.
		🖓 Log Adjacency Changes 🦳 Log Adjacency Change Details
		Administrative Route Distances
a	- Anno Terrat	Inter Area (distance for all intro Area (distance for all routes External (distance for all routes from other routing domains, from other routing domains, another area) key routing domains, key routing domains, key routing domains, key routing domains, routing domains, key routing domains, routing domains, routing domains, routing domains, key routing domains, routing doma
		110 110 110
		Timers (in seconds)
		SPF Delay Time (between when SPF Held Time (between two LSA Group Parang General et when OOPF receives a beyology change and when it starts a SPF calculation) SPF calculations group and refreated)
		5 [10
		Detxuit information Originale
		Configure this to generate default external route into an OSPF routing domain.
		🖵 Enable Default Information Originate 🖉 Winners information this default racts
		Mitter Volue Mitter Types (2014) Route Maps

Resource Management

Cisco ASDM allows administrators to manage the resources for ACLs in Multiple Security Contexts Mode. Resources, such as ACL memory pool or ACL tree instances, which are used when compiling ACLs, can be assigned to security contexts by the administrator to optimize resource usage.



Figure 6. Resource Manager for ACL Memory Pool in Cisco ASDM

Enhanced Monitoring and Reporting Tools Enable Valuable Business-Critical Analysis

Syslog to Access Rule Correlation

Cisco ASDM includes a Syslog to Access Rule Correlation tool that greatly enhances day-to-day security management and troubleshooting activities. With this dynamic tool, security administrators can quickly resolve common configuration issues, along with most user and network connectivity problems. With ASDM 5.2F, users can select a syslog message within the Real-Time Syslog Viewer panel, and by simply clicking the "Create" button at the top of the panel (Figure 7), can invoke the access-control options for that specific syslog. Intelligent defaults help ensure that the configuration process is simple, which helps improve operational efficiency and response times for

business-critical functions. The Syslog to Access Rule Correlation tool also offers an intuitive view into syslog messages invoked by user-configured access rules. Administrators can closely observe enterprise traffic patterns and monitor resource access behavior. Figure 7 indicates the Syslog to Access Rule Correlation capability where a user has selected a syslog message, and has clicked on the Create button to define policies for that flow.

			23.62.20			-		
		HEA Copy	and a second second	and the second second	Color Settings			
	Filter Dy:			-	Show Fill Fin		٩,	
	Severty D	te	Time	Sysing ID	Source P	Destruction P	Description	
	4.8 0	t 27 2006	14:54:22	302013	171.69.47.191	172.23.82.20	Bult inbound TCP connection 0 for inside 171 69.47 191/3943 (171 89.47 191/3943) 1	
		1 27 2006	14:54:09	302014	171.69.47.191	172.23.62.20	Teardown TCP connection 0 for inside: 171.89.47 191/9942 to inside: 172.23.62 2944	
		t 27 2006 t 27 2006	14:54:09	111009 605005	171.69.47.191	172.23.62.20	User "enable_15" executed crist: show logging asitm Login permitted trew 171 69 47.191.094216 inside:172.23 62.20/https:/for.user "enable"	
		1 27 2006	14.54.09	302013	171.69.47.191	172.23.62.20	Bull inbound TCP connection 0 for inside 171.68.47.191/3942 (171.68.47.191/3942) 1	
		1 27 2006	14:54:05	302014	171.69.47.191	172.23.62.20	Teardown TCP connection 0 for intide 171.69.47 191/9941 to inside 172.23.62.20144	
		t 27 2006 t 27 2006	14:54:05	111009	171 00 17 101	133.00.00.00	User 'enable_15' executed crist, show logging asdw	
		1 27 2006	14.54.05	605005 302013	171.69.47.191	172.23.82.20	Login permitted from 171.69.47.191/3941 to inside 172.23.62.20/https for user "enabl Built inbound TCP connection 0 for inside 171.69.47.191/3941 (171.69.47.191/3941) (
		1 27 2006	14:54:02	302014	171.69.47 191	172.23.82.20	Teardown TCP connection 0 for inside 171 69 47 191/3940 to inside 172 23 62 20/44	
		1 27 2006	14:54:02	111009			User 'enable_15' executed crist show wp	
		1 27 2006 1 27 2006	14:54:02	605005 302013	171.69.47.191	172.23.82.20	Login permitted train 171 88.47.191/3940 to inside 172.23.62 20/https: for user "enviol Built inbound TCP connection 0 for inside 171.69.47.191/3940 (171.69.47.191/3940) t	
		1 27 2006	14:50:37	302010	and appendix		2 in use, 0 most used	
		1 27 2006	14:40:38	302010			2 in use, 0 most used	
un los estinos		2006	14:38:44	302014 302013	172.23.116.136	172.23.82.20	Teardown TCP connection 0 for inside: 172 23 116 136/4185 to inside 172 23 62 201	
xplanation,		2006	14:38:28	302013	1/2.23.116.136	172.23.62.20	Euith inbound TCP connection 0 for inside 172 23.116.136/4185 (172 23.116.136/4185 2 in use, 9 most used	
ecommenda	ation	2006	14,20:35	302010			2 in use, 0 most used	
	ACION 1	2006	14:10:35	302010			2 in use, 0 most used	
nd Detail		2006	14.00:35	302010			2 in use 0 most used	
	Explanation		vied Action				rta Reliane) - 172-23.62.20	
	Explanation				File View Tools	Waxwels Holp	Search: AAA Prod	- Curr
	Exploration				File View Tools	Waxwels Holp		- 600
	Explanation				File View Tools	Waren Hele	Search AAA. Prod Process O Data O Financia Q Rohesh 🕁 Sear 🍞 Hele The Prod J. Ro 🐘 · Q Find Chargen Addresses Search	-40.00 (CA
		0 8			File View Tools	Honoris Help Indigension II N Add - III II - Add State:	Search AAA Pro- starrog Dask Direct Contracts Search AAA Pro- Search AAAA Pro- Search AAAA Pro- Search AAAA Pro- Search AAAA Pro- Search	-40.00 (CA
		0 8			File View Tools (5) none (6) bitartaces (6)	Mitantis Hele Infiguration () N Add - () N I Add Static () Add Dynam	Statuto Figure 1 Q Refresh Statu Product <	-40.00 (CA
itart by Choo	osing	0 8			File View Tools Shows Reg of Harrisons Security Policy	Manda Hele Add - W Market - Add - W Market - Add Jackstone - Add Jackstone - Add Jackstone - Add Jackstone - Add Jackstone - Add Jackstone 	Statuto Figure 1 Reference 2 Statuto Procession Procession <td></td>	
	osing	0 8			File View Tools Shares Startscen Security Folloy	Witness Hele Infiguration M M Add + M Add Static Add Dynam Add Nat E H Add Static Add Static	Search AAA Pro- Pro- Pro- Pro- Pro- Pro- Pro- Pro-	- 11
itart by Choo	osing	0 8			File View Tools man and tools bitantaces Security Policy MAT	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Seguri AAA net Seguri AAA net	
itart by Choo	osing	0 8			File View Tools Toom Of Tools Harrisons Security Policy MAT +25	Witness Hele Infiguration M M Add + M Add Static Add Dynam Add Nat E H Add Static Add Static	Stearch AAA Prod Pattering Disk: Prove Pattering Disk Disk Pattering Disk Disk Disk Disk Disk Disk Disk Disk	
itart by Choo	osing	0 8			File View Tools Tools I for the second of t	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Search AAA Prod Patering Disk: Prove Paterink Son Proje The Paterink Son Project Paterink Son Project Paterink Son Paterink Paterink Son Project Paterink Son Paterink Paterink Pateri	ct Groupe
itart by Choo	osing	0 8			File View Tools Trans Of Con- Barrisces Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Seguri AAA net Relating to Data Prove Provided AAA net Relation Provided AAA net Relation Provided AAAA net Relation Provided AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	ct Groupe
itart by Choo	osing	0 8			Pile View Tools Construction Harrisons Security Policy Bit Security Policy Bit Bit Bit Bit Bit Bit Bit Bit	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Search AAA Ped Patrong Dask Prove Reference Sover Proje The State Prove Reference Sover Proje Reference Reference	ct Groups
itart by Choo	osing	0 8			Pile View Tools Tool	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Segun AAA ned Netrog Data Prove Charles Sever Projections Address Data Netro Provided Address Data N	ct Groups sects e retwork retwork
itart by Choo	osing	0 8			Pile View Tools Construction Harrisons Security Policy Bit Security Policy Bit Bit Bit Bit Bit Bit Bit Bit	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Search AAA Ped Peterson Parison Peressee Peterson Peterso	chocee Gio = 1
itart by Choo	osing	0 8			Pile View Tools Tool	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Segun AAA ned Netrog Data Prove Charles Sever Projections Address Data Netro Provided Address Data N	eretwork 2 et Groupe eretwork 3 5 6
itart by Choo	osing	0 8			Pile View Tools Tool	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Seguri AAA ned Netrong Data Prove AAA ned Seguri AAA ned Se	eretwork 2 et Groupe eretwork 3 5 6
itart by Choo	osing	0 8			Pile View Tools Tool	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Seguri AAA ned Netrong Data Prove AAA ned Seguri AAA ned Se	eretwork 2 et Groupe eretwork 3 5 6
itart by Choo	osing	0 8			Pile View Tools	Wards Me Configuration He Hold - Configuration Head	Seguri AAA ned Netrong Data Prove AAA ned Seguri AAA ned Se	eretwork 2 et Groupe eretwork 3 5 6
itart by Choo	osing	0 8			Pile View Tools	Warnets Help anfiguration P N 4 Add - I Tool 4 Add State Add Dynam Add State Add A	Seguri AAA ned Netrorg Data Prove Professionation Professionation Professionation Not Take Inst Take Not Tak Not Tak Not Take Not Tak Not Tak Not Take Not Take Not Taka Not Take Not T	eretwork 2 et Groupe eretwork 3 5 6
itart by Choo	osing	0 8			Pile View Tools	Wards Me Configuration He Hold - Configuration Head	Search AAA Net Netrong C Dati C Funder C Son P He Record C C C C C C C C C C C C C C C C C C C	eretwork 2 et Groupe eretwork 3 5 6
itart by Choo	osing	0 8			Pile View Tools	Moran Per Configuration Per Configuration Co	Seguri AAA ned Netrorg Data Prove Professionation Professionation Professionation Not Take Inst Take Not Tak Not Tak Not Take Not Tak Not Tak Not Take Not Take Not Taka Not Take Not T	eretwork 2 et Groupe eretwork 3 5 6

Figure 7. Syslog to Access Rule Correlation Tool

Syslogs Parsed and Displayed

Monitoring Tools

Cisco ASDM offers in-depth monitoring and reporting services in addition to the at-a-glance monitoring capabilities on the new homepage (Figure 8). Versatile analysis tools create graphical summary reports showing real-time usage, security events, and network activity. Data from each graphical report can be displayed in customizable increments, where a user can choose either a 10-second snapshot or analysis over an extended timeline. The ability to view multiple graphs simultaneously allows users to perform detailed evaluations in parallel. Graphs can be conveniently bookmarked, and data can be exported for future access.

Figure 8. Advanced Monitoring Options with Customizable Graphs



- System Graphs—Provide detailed status information on the Cisco FWSM, including used and free blocks, current memory utilization, and CPU utilization.
- Connection Graphs—Track real-time session and performance monitoring data for connections; address translations; authentication, authorization, and accounting (AAA) transactions; URL filtering requests; and more, on a per-second basis. Connection graphs enable administrators to stay fully informed of their network connections and activities, without being overwhelmed.
- Attack Protection System Graphs—Provide 16 different graphs to display potentially malicious activity. Attack signature information displays activity such as IP, Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), TCP attacks, and Portmap requests.
- Interface Graphs—Provide real-time monitoring of bandwidth usage for each interface on the security appliance. Bandwidth usage is displayed for incoming and outgoing communications. Users can view packet rates, counts, and errors, as well as bit, byte, and collision counts.

Table 1 provides an overall feature summary of Cisco ASDM Version 5.0F.

Complete Cisco FWSM Version 3.2 Feature Support				
Dynamic Dashboard	Detailed device and licensing information Real-time system and traffic profiling Customizable syslog monitoring Real-time device monitoring			
Web-Based Architecture	Advanced Application and Protocol Inspection Configuration			
Up to 80 simultaneous ASDM HTTPS connections	Web GUI for Modular Policy Framework			
Downloadable Cisco ASDM Launcher	Streamlined policy creation provides easy access to all items needed for ACL management, including easy object group creation/modification/viewing, and a policy visualizer.			

 Table 1.
 Cisco ASDM Version 5.2F Overall Feature Summary

Demo Mode supported	 Policy query capability gives administrators advanced search capabilities for their ACLs New object group selector panel enables rapid editing of all network and service object groups
Rich Syslog Support	Robust Security Features
Syslog to ACE (Access Control Element) correlation and instant viewing of syslogs being generated based on a selected ACL	HTTPS authentication proxy for administrative access
Create opposite ACE based on syslog entry	16 levels of user authorization
Search on any text in syslog table	Local authentication database
Many customizations	RADIUS or TACACS authentication support
Rule table and syslog integration enables single-click rule creation from syslog and provides explanation of syslog messages and recommended actions.	
New syslog viewer provides syslog parsing for customizable views based on time, date, syslog IDs, IP addresses, and coloring of logs based on severity.	
World-Class Management of Virtualized Security Services	Flexible Configuration and Software Image Management
Create security policies, logical interfaces, and administrative domains for	Effective file management with directories
multiple virtual firewalls (security contexts)	Direct upload from desktop to FWSM
Resource Manager	Scheduled or immediate reload of FWSM image
Context caching	

Note: Cisco ASDM Version 5.2F is used to configure and manage the new features in FWSM Software Version 3.2.

Cisco ASDM Version 5.0F incorporates all of the features from Cisco ASDM Version 5.0 that are applicable to the Cisco FWSM. All Cisco FWSM Software Version 3.1 features are configurable with Cisco ASDM Version 5.0F except IPv6, which requires CLI configuration.

Licensing

Cisco ASDM Version 5.2F is included with Cisco FWSM Software Version 3.2.

Cisco ASDM Version 5.0F is included with Cisco FWSM Software Version 3.1.

Cisco PIX Device Manager Version 4.1 is included with Cisco FWSM Software Version 2.2 and 2.3.

Cisco PIX Device Manager Version 2.1 is included with Cisco FWSM Software Version 1.1.

User System Requirements

Hardware

- Processor: Pentium 4, AMD Athlon or equivalent
- RAM: 512 MB (minimum) for Microsoft Windows and Sun SPARC, 256MB (minimum) for Red Hat Linux
- Display Resolution: 1024 x 768 pixels (minimum)
- Display Colors: 256 (16-bit high color recommended)

Software

Table 2 lists the operating systems and Web browsers supported by Cisco ASDM Version 5.0.

Table 2. Supported Operating Systems and Web Browsers

Operating Systems	Browsers
Windows 2000 with Service Pack 4, Windows XP (English/Japanese version)	Microsoft Internet Explorer 6.0 with Java 1.4.2 or 1.5 Firefox 1.5 with Java 1.4.2 or 1.5
Sun SPARC Solaris 2.8 or 2.9	Firefox 1.5 with Java 1.4.2 or 1.5
RedHat Desktop, RedHat Enterprise Linux WS 3.0	Firefox 1.5 with Java 1.4.2 or 1.5 GNOME or KDE desktop environment

Note: Cisco ASDM Version 5.0F does not support Windows 95, Windows 98, Windows ME, Windows NT, or the Macintosh operating system.

Additional Information

For more information, please visit the following links.

- Cisco ASDM: <u>http://www.cisco.com/go/asdm</u>
- Cisco FWSM:

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html

Cisco ASA 5500 Series Adaptive Security Appliances: <u>http://www.cisco.com/go/asa</u>



Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA www.cisco.com Tel: 408 526-4000 800 553-NETS (6387)

Fax: 408 527-0883

Asia Pacific Headquarters Cisco Systems, Inc. 168 Robinson Road #28-01 Capital Tower Singapore 068912 www.cisco.com Tei.+85 6317 7777 Fax: +65 6317 7799 Europe Headquarters Cisco Systems International BV Haarlerbergpark Haarlerbergweg 13-19 1101 CH Amsterdam The Netherlands www-europe cisco.com Tel: +31 0 800 020 0791 Fax: +31 0 20 357 1100

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.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iD Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0609R)

Printed in USA

C78-340998-01 12/06