Cisco ASDM Release Notes Version 6.0(2)

May 2008

This document contains release information for Cisco ASDM Version 6.0(2) on Cisco PIX 500 series and Cisco ASA 5500 adaptive series security appliances Version 8.0(2). It includes the following sections:

Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco PIX 500 and ASA 5500 adaptive series security appliances through an intuitive, easy-to-use, web-based management interface. Bundled with supported security appliances, the device manager accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by Cisco PIX 500 and ASA 5500 adaptive series security appliance software Version8.0(2). Its secure, web-based design enables anytime, anywhere access to security appliances.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

New Features

Released: June 18, 2007

Table 1 lists the new features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2).

Note There was no 8.0(1)/6.0(1) release.

Table 1 New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2)

Feature	Description
Routing Features	
EIGRP routing	The security appliance supports EIGRP or EIGRP stub routing.
High Availability Features	
Remote command execution in Failover pairs	You can execute commands on the peer unit in a failover pair without having to connect directly to the peer. This works for both Active/Standby and Active/Active failover.
CSM configuration rollback support	Adds support for the Cisco Security Manager configuration rollback feature in failover configurations.
Failover pair Auto Update support	You can use an Auto Update server to update the platform image and configuration in failover pairs.
Stateful Failover for SIP signaling	SIP media and signaling connections are replicated to the standby unit.
Redundant interfaces	A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to eight redundant interface pairs.
Module Features	
Virtual IPS sensors with the AIP SSM	The AIP SSM running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.
Password reset	You can reset the password on the SSM hardware module.
VPN Authentication Features[1]	
Combined certificate and username/password login	An administrator requires a username and password in addition to a certificate for login to SSL VPN connections.
Internal domain username/password	Provides a password for access to internal resources for users who log in with credentials other than a domain username and password, for example, with a one-time password. This is a password in addition to the one a user enters when logging in.
Generic LDAP support	This includes OpenLDAP and Novell LDAP. Expands LDAP support available for authentication and authorization.

Table 1 New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)

Feature	Description
Onscreen keyboard	The security appliance includes an onscreen keyboard option for the login page and subsequent authentication requests for internal resources. This provides additional protection against software-based keystroke loggers by requiring a user to use a mouse to click characters in an onscreen keyboard for authentication, rather than entering the characters on a physical keyboard.
SAML SSO verified with RSA Access Manager	The security appliance supports Security Assertion Markup Language (SAML) protocol for Single Sign On (SSO) with RSA Access Manager (Cleartrust and Federated Identity Manager).
NTLMv2	Version 8.0(2) adds support for NTLMv2 authentication for Windows-based clients.
Certificate Features	
Local certificate authority	Provides a certificate authority on the security appliance for use with SSL VPN connections, both browser- and client-based.
OCSP CRL	Provides OCSP revocation checking for SSL VPN.
Cisco Secure Desktop Features	
Host Scan	As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection, the remote computer scans for a greatly expanded collection of antivirus and antispyware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the security appliance. The security appliance uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP). With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements. Cisco can provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop.
Simplified prelogin assessment and periodic checks	Cisco Secure Desktop now simplifies the configuration of prelogin and periodic checks to perform on remote Microsoft Windows computers. Cisco Secure Desktop lets you add, modify, remove, and place conditions on endpoint checking criteria using a simplified, graphical view of the checks. As you use this graphical view to configure sequences of checks, link them to branches, deny logins, and assign endpoint profiles, Cisco Secure Desktop Manager records the changes to an XML file. You can configure the security appliance to use returned results in combination with many other types of data, such as the connection type and multiple group settings, to generate and apply a DAP to the session.
VPN Access Policy Features	

Table 1 New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)

Feature	Description
Dynamic access policies (DAP)	VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration. Dynamic Access Policies (DAP) on the security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.
Administrator differentiation	Lets you differentiate regular remote access users and administrative users under the same database, either RADIUS or LDAP. You can create and restrict access to the console via various methods (TELNET and SSH, for example) to administrators only. It is based on the IETF RADIUS service-type attribute.
Platform Enhancements	
VLAN support for remote access VPN connections	Provides support for mapping (tagging) of client traffic at the group or user level. This feature is compatible with clientless as well as IPsec and SSL tunnel-based connections.
VPN load balancing for the ASA 5510	Extends load balancing support to ASA 5510 security appliances that have a Security Plus license.
Crypto conditional debug	Lets users debug an IPsec tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPSec operations and reducing the amount of debug output, you can better troubleshoot the security appliance with a large number of tunnels.
Browser-based SSL VPN Features	
Enhanced portal design	Version 8.0(2) includes an enhanced end user interface that is more cleanly organized and visually appealing.
Customization	Supports administrator-defined customization of all user-visible content.
Support for FTP	You can provide file access via FTP in additional to CIFS (Windows-based).
Plugin applets	Version 8.0(2) adds a framework for supporting TCP-based applications without requiring a pre-installed client application. Java applets let users access these applications from the browser-enabled SSL VPN portal. Initial support is for TELNET, SSH, RDP, and VNC.

Table 1 New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)

Feature	Description
Smart tunnels	A smart tunnel is a connection between an application and a remote site, using a browser-based SSL VPN session with the security appliance as the pathway. Version 8.0(2) lets you identify the applications to which you want to grant smart tunnel access, and lets you specify the path to the application and the SHA-1 hash of its checksum to check before granting it access. Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access. The remote host originating the smart tunnel connection must be running Microsoft Windows Vista, Windows XP, or Windows 2000, and the browser must be enabled with Java, Microsoft ActiveX, or both.
RSS newsfeed	Administrators can populate the clientless portal with RSS newsfeed information, which lets company news or other information display on a user screen.
Personal bookmark support	Users can define their own bookmarks. These bookmarks are stored on a file server.
Transformation enhancements	Adds support for several complex forms of web content over clientless connections, including Adobe flash and Java WebStart.
IPv6	Allows access to IPv6 resources over a public IPv4 connection.
Web folders	Lets browser-based SSL VPN users connecting from Windows operating systems browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.
Microsoft Sharepoint enhancement	Extends Web Access support for Microsoft Sharepoint, integrating Microsoft Office applications available on the machine with the browser to view, change, and save documents shared on a server. Version 8.0(2) supports Windows Sharepoint Services 2.0 in Windows Server 2003.
HTTP/HTTPS Proxy Features	
PAC support	Lets you specify the URL of a proxy autoconfiguration file (PAC) to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL.
Proxy exclusion list	Lets you configure a list of URLs to exclude from the HTTP requests the security appliance can send to an external proxy server.
VPN Network Access Control Features	
SSL VPN tunnel support	The security appliance provides NAC posture validation of endpoints that establish AnyConnect VPN client sessions.
Support for audit services	You can configure the security appliance to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server uses the host IP address to challenge the host directly to assess its health. For example, it might challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host. If the token indicates the remote host is healthy, the posture validation server sends a network access policy to the security appliance for application to the traffic on the tunnel.

Table 1 New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)

Feature	Description
Application Inspection Features	
Modular policy framework inspect class map	Traffic can match one of multiple match commands in an inspect class map; formerly, traffic had to match all match commands in a class map to match the class map.
AIC for encrypted streams and AIC Arch changes	Provides HTTP inspection into TLS, which allows AIC/MPF inspection in WebVPN HTTP and HTTPS streams.
TLS Proxy for SCCP and SIP[2]	Enables inspection of encrypted traffic. Implementations include SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with the Cisco CallManager.
SIP enhancements for CCM	Improves interoperability with CCM 5.0 and 6.x with respect to signaling pinholes.
IPv6 support for SIP	The SIP inspection engine supports IPv6 addresses. IPv6 addresses can be used in URLs, in the Via header field, and SDP fields.
Full RTSP PAT support	Provides TCP fragment reassembly support, a scalable parsing routine on RTSP, and security enhancements that protect RTSP traffic.
Access List Features	
Enhanced service object group	Lets you configure a service object group that contains a mix of TCP services, UDP services, ICMP-type services, and any protocol. It removes the need for a specific ICMP-type object group and protocol object group. The enhanced service object group also specifies both source and destination services. The access list CLI now supports this behavior.
Ability to rename access list	Lets you rename an access list.
Live access list hit counts	Includes the hit count for ACEs from multiple access lists. The hit count value represents how many times traffic hits a particular access rule.
Attack Prevention Features	
Set connection limits for management traffic to the security appliance	For a Layer 3/4 management class map, you can specify the **set connection** command.
Threat detection	You can enable basic threat detection and scanning threat detection to monitor attacks such as DoS attacks and scanning attacks. For scanning attacks, you can automatically shun attacking hosts. You can also enable scan threat statistics to monitor both valid and invalid traffic for hosts, ports, protocols, and access lists.
NAT Features	
Transparent firewall NAT support	You can configure NAT for a transparent firewall.
Monitoring Features	
Secure logging	You can enable secure connections to the syslog server using SSL or TLS with TCP, and encrypted system log message content. Not supported on the PIX series security appliance.
ASDM Features	
Redesigned Interface	Reorganizes information to provide greater logical consistency and ease of navigation.
Expanded onscreen help	ASDM describes features and configuration options on screen, which reduces the need to consult other information sources.
Visual policy editor	The visual policy editor lets an administrator configure access control policies and posture checking.

Table 1 New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)

Feature	Description
Firewall Dashboard	From the home page, you can now track threats to your network by monitoring traffic that exceeds rate limits, as well as allowed and dropped traffic by host, access list, port, or protocol.
Accessibility Features	Features such as keyboard navigation, alternate text for graphics, and improved screen reader support have been added.
Complex Configuration Support	You can move between panes without applying changes, allowing you to enter multi-pane configurations before applying that configuration to the device.
Device List	ASDM maintains a list of recently accessed devices, allowing you to switch between devices and contexts.
SSL VPN configuration wizard	The new SSL VPN configuration wizard provides step-by-step guidance in configuring basic SSL VPN connections.
Startup Wizard Enhancement	The Startup Wizard now allows you to configure the adaptive security appliance to pass traffic to an installed CSC SSM.
ASDM Assistant Enhancements‘	An assistant for configuring Secure Voice was added.
Packet Capture Wizard	The Packet Capture Wizard assists you in obtaining and downloading sniffer trace in PCAP format.
Service Policy Rule Wizard	Updated to support IPS Virtualization.
Certificate Management Enhancements	The certificate management GUI is reorganized and simplified.

1. Clientless SSL VPN features are not supported on the PIX security appliance.
2. TLS proxy is not supported on the PIX security appliance.

ASDM Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for ASDM Version 6.0(2).

Table 2 Operating System and Browser Requirements

Operating System	Version	Browser	Other Requirements
Microsoft Windows[1]	Windows Vista Windows 2003 Server Windows XP Windows 2000 (Service Pack 4)	Internet Explorer 6.0 or 7.0 with Sun Java SE[2] Plug-in 1.4.2, 5.0 (1.5.0), or 6.0 Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Note We support both the English and Japanese versions of Windows.		**Note** **HTTP 1.1**—Settings for **Internet Options > Advanced > HTTP 1.1** should use HTTP 1.1 for both proxy and non-proxy connections.	
Apple MacIntosh	Apple MacIntosh OS X	Firefox 1.5 or 2.0 or Safari 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 4 running GNOME or KDE	Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	

1. ASDM is not supported on Windows 3.1, Windows 95, Windows 98, Windows ME, or Windows NT4.
2. Obtain Sun Java from http://www.java.com/en/download/manual.jsp.

Memory Errors in Firefox

Firefox may stop responding or give an out of memory error message Linux and Windows if multiple instances of ASDM are running. You can use the following steps to increase the Java memory and work around the behavior.

This section describes how to increase the memory for Java on the following platforms:

- Java Plug-In for Windows
- Java Plug-In on Linux

Java Plug-In for Windows

To change the memory settings of the Java Plug-in on Windows for Java Plug-in versions 1.4.2 and 1.5, perform the following steps:

Step 1 Exit all browsers.

Step 2 Click **Start > Settings > Control Panel**.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click **Java Plug-in**. The Java Plug-in Control Panel appears.

b. Click the **Advanced** tab.

c. Type **-Xmx256m** in the Java RunTime Parameters field.

d. Click **Apply** and exit the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click **Java**. The Java Control Panel appears.

b. Click the **Java** tab.

c. Click **View** under Java Applet Runtime Settings. The Java Runtime Settings Panel appears.

d. Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.

e. Click **OK** and exit the Java Control Panel.

Java Plug-In on Linux

To change the settings of Java Plug-in version 1.4.2 or 1.5 on Linux, perform the following steps:

Step 1 Exit all browsers.

Step 2 Open the Java Plug-in Control Panel by launching the Control Panel executable file.

Note In the Java 2 SDK, this file is located in SDK installation directory/jre/bin/ControlPanel. For example: if the Java 2 SDK is installed at /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel. In a Java 2 Runtime Environment installation, the file is located at JRE installation directory/bin/ControlPanel.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click the **Advanced** tab.

b. Type **-Xmx256m** in the Java RunTime Parameters field.

c. Click **Apply** and close the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click the **Java** tab.

b. Click **View** under Java Applet Runtime Settings.

c. Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.

d. Click **OK** and exit the Java Control Panel.

Supported Platforms and Feature Licenses

This software version supports the following platforms; see the associated tables for the feature support for each model:

- ASA 5505, Table 3
- ASA 5510, Table 4
- ASA 5520, Table 5
- ASA 5540, Table 6
- ASA 5550, Table 7
- PIX 515/515E, Table 8
- PIX 525, Table 9
- PIX 535, Table 10

Note Items that are in italics are separate, optional licenses that you can replace the base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 WebVPN license plus the GTP/GPRS license; or all four licenses together.

Table 3 ASA 5505 Adaptive Security Appliance License Features

ASA 5505	Base License		Security Plus	
Users, concurrent[1]	10	*Optional Licenses:*	10	*Optional Licenses:*
		50 *Unlimited*		*50* *Unlimited*
Security Contexts	No support		No support	
VPN Sessions[2]	10 combined IPSec and WebVPN		25 combined IPSec and WebVPN	
Max. IPSec Sessions	10		25	
Max. WebVPN Sessions	2	*Optional License: 10*	2	*Optional License: 10*
VPN Load Balancing	No support		No support	
TLS Proxy for SIP and Skinny Inspection	Supported		Supported	
Failover	None		Active/Standby (no stateful failover)	
GTP/GPRS	No support		No support	
Maximum VLANs/Zones	3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)		20	
Maximum VLAN Trunks	No support		Unlimited	
Concurrent Firewall Conns[3]	10 K		25 K	
Max. Physical Interfaces	Unlimited, assigned to VLANs/zones		Unlimited, assigned to VLANs/zones	
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*	Base (DES)	*Optional license: Strong (3DES/AES)*
Minimum RAM	256 MB		256 MB	

1. In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit only when they communicate with the outside (Internet VLAN). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host command** to view the host limits.
2. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
3. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Table 4 ASA 5510 Adaptive Security Appliance License Features

ASA 5510	Base License					Security Plus					
Users, concurrent	Unlimited					Unlimited					
Security Contexts	No support					2	*Optional Licenses:*				
							5				
VPN Sessions[1]	250 combined IPSec and WebVPN					250 combined IPSec and WebVPN					
Max. IPSec Sessions	250					250					
Max. WebVPN Sessions	2	*Optional Licenses:*					2	*Optional Licenses:*				
		10	*25*	*50*	*100*	*250*		*10*	*25*	*50*	*100*	*250*
VPN Load Balancing	No support						No support					
TLS Proxy for SIP and Skinny Inspection	Supported						Supported					
Failover	None						Active/Standby or Active/Active					
GTP/GPRS	No support						No support					
Max. VLANs	50						100					
Concurrent Firewall Conns[2]	50 K						130 K					
Max. Physical Interfaces	Unlimited						Unlimited					
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*					Base (DES)	*Optional license: Strong (3DES/AES)*				
Min. RAM	256 MB						256 MB					

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 5 ASA 5520 Adaptive Security Appliance License Features

ASA 5520	Base License				
Users, concurrent	Unlimited				Unlimited
Security Contexts	2	*Optional Licenses:*			
		5	10	20	
VPN Sessions[1]	750 combined IPSec and WebVPN				
Max. IPSec Sessions	750				

Table 5 ASA 5520 Adaptive Security Appliance License Features (continued)

ASA 5520	Base License											
Max. WebVPN Sessions	2	*Optional Licenses:*										
		10	*25*	*50*	*100*	250	*500*	*750*				
VPN Load Balancing	Supported											
TLS Proxy for SIP and Skinny Inspection	Supported											
Failover	Active/Standby or Active/Active											
GTP/GPRS	None	*Optional license: Enabled*										
Max. VLANs	150											
Concurrent Firewall Conns[2]	280 K											
Max. Physical Interfaces	Unlimited											
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*										
Min. RAM	512 MB											

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 6 ASA 5540 Adaptive Security Appliance License Features

ASA 5540	Base License								
Users, concurrent	Unlimited					Unlimited			
Security Contexts	2	Optional licenses:							
		5	*10*	*20*	*50*				
VPN Sessions[1]	5000 combined IPSec and WebVPN								
Max. IPSec Sessions	5000								
Max. WebVPN Sessions	2	*Optional Licenses:*							
		10	*25*	*50*	*100*	250	*500*	*750*	*1000*	*2500*
VPN Load Balancing	Supported								
TLS Proxy for SIP and Skinny Inspection	Supported								
Failover	Active/Standby or Active/Active								
GTP/GPRS	None	*Optional license: Enabled*							
Max. VLANs	200								
Concurrent Firewall Conns[2]	400 K								
Max. Physical Interfaces	Unlimited								
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*							
Min. RAM	1 GB								

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.

2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 7 ASA 5550 Adaptive Security Appliance License Features

ASA 5550	Base License									
Users, concurrent	Unlimited									
Security Contexts	2	Optional licenses:								
		5	*10*	*20*	*50*					
VPN Sessions[1]	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2	*Optional Licenses:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	5000
VPN Load Balancing	Supported									
TLS Proxy for SIP and Skinny Inspection	Supported									
Failover	Active/Standby or Active/Active									
GTP/GPRS	None	*Optional license: Enabled*								
Max. VLANs	250									
Concurrent Firewall Conns[2]	650 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*								
Min. RAM	4 GB									

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 8 PIX 515/515E Security Appliance License Features

PIX 515/515E	R (Restricted)	UR (Unrestricted)	FO (Failover)[1]	FO-AA (Failover Active/Active)[1]
Users, concurrent	Unlimited	Unlimited	Unlimited	Unlimited
Security Contexts	No support	2 Optional license: 5	2 Optional license: 5	2 Optional license: 5
IPSec Sessions	2000	2000	2000	2000
WebVPN Sessions	No support	No support	No support	No support
VPN Load Balancing	No support	No support	No support	No support
TLS Proxy for SIP and Skinny Inspection	No support	No support	No support	No support

Table 8 PIX 515/515E Security Appliance License Features (continued)

PIX 515/515E	R (Restricted)			UR (Unrestricted)			FO (Failover)[1]			FO-AA (Failover Active/Active)[1]		
Failover	No support			Active/Standby Active/Active			Active/Standby			Active/Standby Active/Active		
GTP/GPRS	None	*Optional license: Enabled*		None	*Optional license: Enabled*		None	*Optional license: Enabled*		None	*Optional license: Enabled*	
Max. VLANs	10			25			25			25		
Concurrent Firewall Conns[2]	48 K			130 K			130 K			130 K		
Max. Physical Interfaces	3			6			6			6		
Encryption	None	*Optional licenses:*		None	*Optional licenses:*		None	*Optional licenses:*		None	*Optional licenses:*	
		Base (DES)	*Strong (3DES/AES)*		*Base (DES)*	*Strong (3DES/AES)*		*Base (DES)*	*Strong (3DES/AES)*		*Base (DES)*	*Strong (3DES/AES)*
Min. RAM	64 MB			128 MB			128 MB			128 MB		

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 9 PIX 525 Security Appliance License Features

PIX 525	R (Restricted)	UR (Unrestricted)	FO (Failover)[1]	FO-AA (Failover Active/Active)[1]
Users, concurrent	Unlimited	Unlimited	Unlimited	Unlimited
Security Contexts	No support	2 Optional licenses: *5 10 20 50*	2 Optional licenses: *5 10 20 50*	2 Optional licenses: *5 10 20 50*
IPSec Sessions	2000	2000	2000	2000
WebVPN Sessions	No support	No support	No support	No support
VPN Load Balancing	No support	No support	No support	No support
TLS Proxy for SIP and Skinny Inspection	No support	No support	No support	No support
Failover	No support	Active/Standby Active/Active	Active/Standby	Active/Standby Active/Active
GTP/GPRS	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*
Max. VLANs	25	100	100	100
Concurrent Firewall Conns[2]	140 K	280 K	280 K	280 K

Table 9 PIX 525 Security Appliance License Features (continued)

PIX 525	R (Restricted)			UR (Unrestricted)			FO (Failover)[1]			FO-AA (Failover Active/Active)[1]		
Max. Physical Interfaces	6			10			10			10		
Encryption	None	*Optional licenses:*		None	*Optional licenses:*		None	*Optional licenses:*		None	*Optional licenses:*	
		Base (DES)	*Strong (3DES/ AES)*		*Base (DES)*	*Strong (3DES/ AES)*		*Base (DES)*	*Strong (3DES/ AES)*		*Base (DES)*	*Strong (3DES/ AES)*
Min. RAM	128 MB			256 MB			256 MB			256 MB		

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 10 PIX 535 Security Appliance License Features

PIX 535	R (Restricted)				UR (Unrestricted)				FO (Failover)[1]				FO-AA (Failover Active/Active)[1]			
Users, concurrent	Unlimited				Unlimited				Unlimited				Unlimited			
Security Contexts	No support				2	*Optional licenses:*			2	*Optional licenses:*			2	*Optional licenses:*		
					5	*10*	*20*	*50*		*5*	*10*	*20*	*50*	*5*	*10*	*20*	*50*
IPSec Sessions	2000				2000				2000				2000			
WebVPN Sessions	No support				No support				No support				No support			
VPN Load Balancing	No support				No support				No support				No support			
TLS Proxy for SIP and Skinny Inspection	No support				No support				No support				No support			
Failover	No support				Active/Standby Active/Active				Active/Standby				Active/Standby Active/Active			
GTP/GPRS	None	*Optional license: Enabled*			None	*Optional license: Enabled*			None	*Optional license: Enabled*			None	*Optional license: Enabled*		
Max. VLANs	50				150				150				150			
Concurrent Firewall Conns[2]	250 K				500 K				500 K				500 K			
Max. Physical Interfaces	8				14				14				14			
Encryption	None	*Optional licenses:*			None	*Optional licenses:*			None	*Optional licenses:*			None	*Optional licenses:*		
		Base (DES)	*Strong (3DES/ AES)*			*Base (DES)*	*Strong (3DES/ AES)*			*Base (DES)*	*Strong (3DES/ AES)*			*Base (DES)*	*Strong (3DES/ AES)*	
Min. RAM	512 MB				1024 MB				1024 MB				1024 MB			

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

ASDM and SSM Compatibility

ASDM Version 6.0(2) supports the following SSMs and releases:

- Advanced Inspection and Prevention (AIP) SSM, software Version 5.0, 5.1, 6.0
- Content Security and Control (CSC) SSM, software Version 6.1
- Advanced Inspection and Prevention (AIP) SSC, Version 6.2

Upgrading ASDM

This section describes how to upgrade ASDM to a new ASDM release. If you have a Cisco.com login, you can obtain ASDM from the following website:

http://www.cisco.com/cisco/software/navigator.html

Note If you are upgrading from PIX Version 6.3, first upgrade to Version 7.0 according to the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*. Then upgrade PDM to ASDM according to the ASDM 5.0 release notes.

If you have a previous release of ASDM on your security appliance and want to upgrade to the latest release, you can do so from within ASDM. We recommend that you upgrade the ASDM image before the platform image. ASDM is backwards compatible, so you can upgrade the platform image using the new ASDM; you cannot use an old ASDM with a new platform image.

To upgrade ASDM, perform the following steps:

Step 1 Download the new ASDM image to your PC.

Step 2 Launch ASDM.

Step 3 From the Tools menu:

a. In ASDM 5.0 and 5.1, click **Upload Image from Local PC**.

b. In ASDM 5.2, click **Upgrade Software**.

Step 4 With ASDM selected, click **Browse Local** to select the new ASDM image.

Step 5 To specify the location in Flash memory where you want to install the new image, enter the directory path in the field or click **Browse Flash**.

If your security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifying the same destination filename. You can rename the image after it was uploaded using the **Tools > File Management** tool.

If you have enough memory for both versions, you can specify a different name for the new version. If you need to revert to the old version, it is still in your Flash memory.

Step 6 Click **Upload Image**.

When ASDM is finished uploading, the following message appears:

"ASDM Image is Uploaded to Flash Successfully."

Step 7 If the new ASDM image has a different name than the old image, then you must configure the security appliance to load the new image in the **Configuration > Properties > Device Administration > Boot System/Configuration** pane.

Step 8 To run the new ASDM image, you must exit ASDM and reconnect.

Step 9 Download the new platform image using the **Tools > Upgrade Software** tool.

To reload the new image, reload the security appliance using the **Tools > System Reload** tool.

Getting Started with ASDM

This section describes how to connect to ASDM and start your configuration. If you are using the security appliance for the first time, your security appliance might include a default configuration. You can connect to a default IP address with ASDM so that you can immediately start to configure the security appliance from ASDM. If your platform does not support a default configuration, you can log in to the CLI and run the **setup** command to establish connectivity. See Before You Begin for more detailed information about networking.

This section includes the following topics:

Before You Begin

If your security appliance includes a factory default configuration, you can connect to the default management address of 192.168.1.1 with ASDM. On the ASA 5500 series adaptive security appliance, the interface to which you connect with ASDM is Management 0/0. For the PIX 500 series security appliance, the interface to which you connect with ASDM is Ethernet 1. To restore the default configuration, enter the **configure factory-default** command at the security appliance CLI.

Make sure the PC is on the same network as the security appliance. You can use DHCP on the client to obtain an IP address from the security appliance, or you can set the IP address to a 192.168.1.0/24 network address.

If your platform does not support the factory default configuration, or you want to add to an existing configuration to make it accessible for ASDM, access the security appliance CLI according to the *Cisco Security Appliance Command Line Configuration Guide*, and enter the **setup** command. The **setup** command prompts you for a minimal configuration to connect to the security appliance using ASDM.

Note You must have an inside interface already configured to use the **setup** command. The Cisco PIX security appliance default configuration includes an inside interface, but the Cisco ASA adaptive security appliance default configuration does not. Before using the **setup** command, enter the **interface gigabitethernet** *slot*/*port* command, and then the **nameif inside** command. The *slot* for interfaces that are built in to the chassis is **0**. For example, enter **interface gigabitethernet 0/1.** The Cisco PIX 500 series and the ASA 5510 adaptive security appliance have an Ethernet-type interface.

Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher is an improvement over running ASDM in a Java Applet. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches faster, and caches previously-entered IP addresses and usernames.

To download the ASDM Launcher, perform the following steps:

Step 1 From a supported web browser on the security appliance network, enter the following URL:

https://*interface_ip_address*

In transparent firewall mode, enter the management IP address.

Note Be sure to enter **https**, not **http**.

Step 2 Click **OK** or **Yes** to all prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

Step 3 Click **Download ASDM Launcher and Start ASDM**.

The installer downloads to your PC.

Step 4 Run the installer to install the ASDM Launcher.

Starting ASDM from the ASDM Launcher

The ASDM Launcher is for Windows only.

To start ASDM from the ASDM Launcher, perform the following steps:

Step 1 Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or start it from the **Start** menu.

Step 2 Enter the security appliance IP address or hostname, your username, and your password, and then click **OK**.

If there is a new version of ASDM on the security appliance, the ASDM Launcher automatically downloads it before starting ASDM.

Using ASDM in Demo Mode

ASDM Demo Mode is available as a separately installed application running under Windows. It makes use of the ASDM Launcher and pre-packaged configuration files to let you run ASDM without having a live device available. ASDM Demo Mode lets you:

- Perform configuration and select monitoring tasks via ASDM as though you were interacting with a real device.
- Demonstrate ASDM or security appliance features using the ASDM interface.
- Perform configuration and monitoring tasks with the Content Security and Control (CSC) SSM.

ASDM Demo Mode provides simulated monitoring data, including real-time system log messages. The data shown is randomly generated, but the experience is identical to what you would see when connecting to a real device.

ASDM Demo Mode has the following limitations:

- Changes made to the configuration will appear in the GUI but are not applied to the configuration file. That is, when you click the **Refresh** button, it will revert back to the original configuration. The changes are never saved to the configuration file.
- File/Disk operations are not supported.
- Monitoring and logging data are simulated. Historical monitoring data is not available.
- You can only log in as an admin user; you cannot log in as a monitor-only or read-only user.
- Demo Mode does not support the following features:
  - File menu:

    Save Running Configuration to Flash

    Save Running Configuration to TFTP Server

    Save Running Configuration to Standby Unit

    Save Internal Log Buffer to Flash

    Clear Internal Log Buffer
  - Tools menu:

    Command Line Interface

    Ping

File Management

Update Image

File Transfer

Upload image from Local PC

System Reload

- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Failover—Configuring a standby device

- These operations cause a reread of the configuration and therefore will revert the configuration back to the original settings.
  - Switching contexts
  - Making changes in the Interface panel
  - NAT panel changes
  - Clock panel changes

To run ASDM in Demo Mode, perform the following steps:

Step 1 If you have not yet installed the Demo Mode application, perform the following steps:

a. Download the ASDM Demo Mode installer from the following website:

http://www.cisco.com/cisco/software/navigator.html

The filename is asdm-demo-*version*.msi.

b. Double-click the installer to install the software.

Step 2 Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or start it from the **Start** menu.

Step 3 Check **Run in Demo Mode**.

Step 4 To set the platform, context and firewall modes, and ASDM Version, click **Demo** and make your selections from the Demo Mode area.

Step 5 To use new ASDM images as they come out, you can either download the latest installer, or you can download the normal ASDM images and install them for Demo Mode:

a. Download the image from the download page (see Step 1).

The filename is asdm-*version*.bin.

b. In the Demo Mode area, click **Install ASDM Image**.

A file browser appears. Find the ASDM image file in the browser.

Step 6 Click **OK** to launch ASDM Demo Mode.

You see a Demo Mode label in the title bar of the window.

Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

Step 1 From a supported web browser on the security appliance network, enter the following URL:

https://*interface_ip_address*

In transparent firewall mode, enter the management IP address.

Note Be sure to enter **https**, not **http**.

Step 2 Click **OK** or **Yes** to all browser prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

Step 3 Click **Run ASDM as a Java Applet**.

Step 4 Click **OK** or **Yes** to all Java prompts, including the name and password prompt. By default, leave the name and password blank.

Using the Startup Wizard

The Startup Wizard helps you easily configure a single mode security appliance or a context in multiple context mode.

To use the Startup Wizard to configure the basic setup of the security appliance, perform the following steps:

Step 1 Launch the wizard according to the steps for the correct security context mode.

- In single context mode, click **Wizards > Startup Wizard**.
- In multiple context mode, for each new context, perform the following steps:
  a. Create a new context using the **System > Configuration > Security Context** pane.
  b. Be sure to allocate interfaces to the context.
  c. When you apply the changes, ASDM prompts you to use the Startup Wizard.
  d. Click the **System/Contexts** icon on the toolbar, and choose the context name.
  e. Click **Wizards > Startup Wizard**.

Step 2 Click **Next** as you proceed through the Startup Wizard screens, filling in the appropriate information in each screen, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.

Step 3 Click **Finish** on the last pane to transmit the configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of the connection changes.

Step 4 Enter other configuration details on the **Configuration** panes.

Using the VPN Wizard

The VPN Wizard configures basic VPN access for LAN-to-LAN or remote client access. The VPN Wizard is available only for security appliances running in single context mode and routed (not transparent) firewall mode.

To use the VPN Wizard to configure VPN, perform the following steps:

Step 1 Click **Wizards > VPN Wizard**.

Step 2 Supply information on each wizard pane. Click **Next** to move through the VPN Wizard panes. You may use the default IPSec and IKE policies. Click **Help** for more information about each field.

Step 3 After you complete the VPN Wizard information, click **Finish** on the last pane to transmit the configuration to the security appliance.

Printing from ASDM

Note Printing is supported only for Microsoft Windows 2000 or XP in this release. There is a known caveat (CSCse15764) for printing from Windows XP that causes printing to be extremely slow.

ASDM supports printing for the following features:

- The Configuration > Interfaces table
- All Configuration > Security Policy tables
- All Configuration > NAT tables
- The Configuration > VPN > IPSec > IPSec Rules table
- Monitoring > Connection Graphs and its related table

ASDM Limitations

This section describes ASDM limitations, and includes the following topics:

Unsupported Commands

ASDM does not support the complete command set of the CLI. In most cases, ASDM ignores unsupported commands, and they can remain in your configuration.

One-Time Password Not Supported

ASDM does not support the one-time password (OTP) authentication mechanism.

Effects of Unsupported Commands

- If ASDM loads an existing running configuration and finds IPv6-related commands, ASDM displays a dialog box informing you that it does not support IPv6. You cannot configure any IPv6 commands in ASDM, but all other configuration is available.
- If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, choose **Options > Show Commands Ignored by ASDM on Device**.
- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.

  Monitor-only mode allows access to the following functions:

  – The **Monitoring** area

  – The CLI tool (**Tools > Command Line Interface**), which lets you use the CLI commands

  To exit Monitor-only mode, use the CLI tool or access the security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.

Note You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to three by your system administrator, which allows Monitor-only mode. For more information, choose **Configuration > Properties > Device Administration > User Accounts** and **Configuration > Properties > Device Administration > AAA Access**.

Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when you add them through the CLI, but that you cannot add or edit in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If the command is view-only, then it appears in the GUI, but you cannot edit it.

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used, except for use in VPN group policy screens
capture	Ignored
established	Ignored

Unsupported Commands	ASDM Behavior
failover timeout	Ignored
ipv6, **any IPv6 addresses**	Ignored
pager	Ignored
pim accept-register route-map	Ignored. You can only configure the **list** option using ASDM.
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored

service-policy global	Ignored if it uses a **match access-list** class. For example:
	`access-list myacl line 1 extended permit ip any any`
	`class-map mycm`
	`match access-list mycl`
	`policy-map mypm`
	`class mycm`
	`inspect ftp`
	`service-policy mypm global`

sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	Ignored
terminal	Ignored
virtual	Ignored

Other CLI Limitations

- ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, you cannot use the following:

  ```
  ip address inside 192.168.2.1 255.255.0.255
  ```

Interactive User Commands Not Supported in ASDM CLI Tool

The ASDM CLI tool does not support interactive user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter "[yes/no]" but does not recognize your input. ASDM then times out waiting for your response.

For example:

1. From the ASDM Tools menu, click **Command Line Interface.**
2. Enter the command: **`crypto key generate rsa`**

   ASDM generates the default 1024-bit RSA key.
3. Enter the command again: **`crypto key generate rsa`**

   Instead of regenerating the RSA keys by overwriting the previous one, ASDM displays the following error:

   ```
   Do you really want to replace them? [yes/no]:WARNING: You already have RSA
   ke0000000000000$A key
   Input line must be less than 16 characters in length.
   ```

```
%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

Workaround:

- You can configure most commands that require user interaction by means of the ASDM panes.
- For CLI commands that have a **noconfirm** option, use this option when entering the CLI command. For example:

  crypto key generate rsa noconfirm

Unsupported Characters

ASDM does not support any non-English characters or any other special characters. If you enter non-English characters in any text entry field, they become unrecognizable when you submit the entry, and you cannot delete or edit them.

If you are using a non-English keyboard or usually type in a language other than English, be careful not to enter non-English characters accidentally.

Workaround:

For workarounds, see CSCeh39437 under Caveats, page 25.

Caveats

The following sections describes the open caveats for Version 6.0(2).

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/l

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats - Version 6.0(2)

The following list shows caveats that are resolved for Version 6.0(2):

Table 11 Open ASDM Caveats

	Software Version 6.0(2)	
ID Number	**Corrected**	**Caveat Title**
CSCsh00014	No	Help not working for IPS ASDM on Linux
CSCsh61229	No	ASDM: AdvEndPt Firewall rules allows conflicting rules to be configured
CSCsi24281	No	ASDM: client cert auth - multiple client certs - popup may lockup
CSCsi39246	No	Refresh arrows turn pink on accessing or leaving various screens
CSCsi49544	No	ASDM: too many steps to add a new customization
CSCsi72634	No	Incorrect help content when toggling between devices
CSCsj00059	No	ASDM:VPN-Session Details, ACL hits not updated even after Refresh
CSCsj07705	No	ASDM: Exception after Deleting Local CA and clicking Reset
CSCsj14583	No	ASDM does not allow spaces in group-policy names
CSCsj16562	No	Show log option from access-rule table not working correctly
CSCsj16580	No	Cannot configure TLS Maximum Sessions via ASDM
CSCsj16920	No	Local CA: leaving/returning while disabled enables blocked fields
CSCsj17114	No	Edit URL bookmarks then cancel. Change is still applied.
CSCsj20946	No	default vlan out of range
CSCsj22326	No	ASDM: Local CA passphrase field should be obscured - not in clear
CSCsj22419	No	Local CA - Enable should be grayed out after Disabling CA
CSCsj22650	No	ASDM won't allow customer to choose vlan on 5505
CSCsj22691	No	Need to provide option to select interface in SLA monitoring
CSCsj22717	No	CSC Home Page graphs time is out of sync with ASA time by one hour.
CSCsj25339	No	ASDM : Unable to edit the default Resource Class through ASDM
CSCsj26284	No	TFW NAT: Selecting IP address browse button twice will freeze panel
CSCsj26304	No	SSL VPN: smart-tunnel changes all entries
CSCsj27201	No	Filtering should search within CSM_INLINE. Should not display CSM_INLINE
CSCsj27897	No	system home resource graphs show all graphs though only 10 are selected.
CSCsj28212	No	File Management: cut/paste: Not working correctly/Panel is not refreshed
CSCsj29060	No	Spurious NAT-T command sent when configuring TCP in IKE Parameters

End-User License Agreement

For information on the end-user license agreement, go to:

https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Related Documentation

For additional information on ASDM or its platforms, see the ASDM online Help or the following documentation found on Cisco.com:

- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Migrating to ASA forVPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Release Notes for Cisco Intrusion Prevention System 5.0*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.0*
- *Release Notes for Cisco Intrusion Prevention System 5.1*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.