Cisco ASDM Release Notes Version 5.2(1)

August 2006

This document contains release information for Cisco ASDM Version 5.2(1) on Cisco PIX 500 series and Cisco ASA 5500 series security appliances Version 7.2(1). 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 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 series security appliance software Version 7.2(1). Its secure, web-based design enables anytime, anywhere access to security appliances.

New Features

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

Released: May 31, 2006

Table 1 lists the new features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1).

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1)

Feature	Description
Platform Features	
ASA 5505 support	The ASA 5505 was introduced in this release. The ASA 5505 is a new model for small office/home office, enterprise teleworker environments, includes a built-in 8-port Fast Ethernet switch, and supports Easy VPN, Dual ISP, and has many more features The ASA 5505 has Power over Ethernet (PoE) switch ports that can be used for PoE devices, such as IP phones. However, these ports are not restricted to that use. They can also be used as Ethernet switch ports. If a PoE device is not attached, power is not supplied to the port.
ASA 5550 support	The ASA 5550 delivers gigabit-class security services and enables Active/Active high availability for large enterprise and service-provider networks in a reliable, 1RU form-factor. Providing gigabit connectivity in the form of both Ethernet- and Fiber-based interfaces with high-density VLAN integration, the ASA 5550 enables businesses to segment their networks into numerous high-performance zones for improved security.
Easy VPN Features (ASA 5505 Only)	
Client Mode (also called Port Address Translation) and Network Extension Mode	• Client Mode—Hides the IP addresses of devices on the ASA 5505 private network, so that all traffic from the ASA 5505 private network arrives on the private network of the central-site security appliance with a single-source, assigned IP address. You cannot ping or access a device on the ASA 5505 private network from the central site, but you can access the assigned IP address. • Network Extension Mode—Permits devices behind the security appliance to have direct access to devices on the ASA 5505 private network only through the tunnel. You can ping or access a device on the ASA 5505 network from the central site. The ASA 5505 does not have a default mode; you must specify the one that you want to use.
Automatic Tunnel Initiation	Supports NEM, but not Client Mode. It uses a group name, username, and password stored in the configuration to initiate the tunnel.
IKE and IPsec Support	The ASA 5505 supports preshared keys and certificates (RSA-SIG). The security appliance uses IKE Aggressive Mode for preshared keys and IKE Main Mode for RSA-SIG based key exchange. Cisco ASA 5505 can initiate IPsec, IPsec over NAT-T, and IPsec over cTCP sessions.
Secure Unit Authentication (SUA)	Supports the ASA 5505 authentication with dynamically generated authentication credentials or with static credentials to be entered at tunnel initiation. With SUA enabled, the user must manually trigger the IKE tunnel using a browser or an interactive CLI.
Individual User Authentication (IUA)	Enables static and one-time password authentication of individual clients on the inside network. IUA and SUA are independent of each other; they work in combination or isolation from each other.
Token-Based Authentication	Supports Security Dynamics (SDI) SecurID one-time passwords.
Authentication by HTTP Redirection	Redirects unauthenticated HTTP traffic to a login page if SUA or a username and password are not configured or if IUA is disabled.

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
Load Balancing	An ASA 5505 configured with dual ISP backup supports cluster-based VPN load balancing over the two Ethernet ports available in the Internet zone. The load-balancing scheme involves a "virtual director" IP address that is the destination of incoming client connections. The server that share a virtual director IP address form a cluster, where one cluster member acts as the cluster master. The master receives a request sent to the virtual director and redirects the client, using a proprietary IKE notify message, to the optimal server in the cluster. The current ISAKMP session terminates, and a new session is attempted to the optimal server. If the connection to the optimal server fails, the client reconnects to the primary server (at the virtual director IP address of the cluster) and repeats the load-balancing procedure. If the connection to the primary server fails, the client rolls over to the next configured backup server, which may be the master of another cluster.
Failover (using Backup Server List)	You can configure a list of 10 backup servers in addition to the primary server. The ASA 5505 attempts to establish a tunnel with the primary server. If that attempt fails, the ASA 5505 attempts to establish a tunnel with other specified servers in the backup server list in sequence.
Device Pass-Through	Encompasses both IP Phone Pass Through and LEAP Pass Through features. Certain devices, such as printers and Cisco IP phones, are incapable of performing authentication, so they cannot participate in IUA. With device pass-through enabled, the ASA 5505 exempts these devices from authentication if IAU is enabled. The Easy VPN Remote feature identifies the devices to exempt, based on a configured list of MAC addresses. A related issue exists with wireless devices such as wireless access points and wireless nodes. These devices require LEAP/PEAP authentication to let wireless nodes participate in the network. It is only after the LEAP/PEAP authentication stage that the wireless nodes can perform IUA. The ASA 5505 also bypasses LEAP/PEAP packets when you enable Device Pass Through, so that the wireless nodes can participate in IUA.
IKE Mode Configuration	You can set the attribute values that the ASA 5505 requests after IKE Phase I and XAUTH. The device at the central site downloads the VPN policy and the ASA 5505 dynamically configures the features based on the security values. Except for SUA, the Clear Save password, and the backup concentrator list, the dynamic feature configuration lasts only while the tunnel is up.
Remote Management	Supports management of the ASA 5505 over the tunnel to the outside interface with NEM configured, and in the clear to the outside interface.
DNS Resolution of Easy VPN Peer Names	The ASA 5505 resolves the Easy VPN peer names with the DNS server. You can specify the DNS name of the server/client in the CLI.
Split tunneling	Allows the client decide which traffic to send over the tunnel, based on a configured list of networks accessible by tunneling to the central site. Traffic destined to a network other than those listed in the split tunnel network list is sent out in the clear. A zero-length list indicates no split tunneling, and all traffic travels over the tunnel.
Push Banner	Allows you to configure a 491-byte banner message to display in HTTP form to individual users who try to authenticate using IUA.
Application Inspection Features	
Enhanced ESMTP Inspection	This feature allows you to detect attacks, including spam, phising, malformed message attacks, and buffer overflow and underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detects several attacks, blocks senders and receivers, and blocks mail relay.

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
DCERPC Inspection	This feature allows you to change the default configuration values used for DCERPC application inspection using a DCERPC inspect map. DCERPC is a protocol used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely. Typically, a client queries a server called the Endpoint Mapper (EPM) that listens on a well-known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance that provides the service. The security appliance allows the appropriate port number and network address and also applies NAT or PAT, if needed, for the secondary connection.
Enhanced NetBIOS Inspection	This feature allows you to change the default configuration values used for NetBIOS application inspection. NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service packets and NetBIOS datagram services packets. It also enforces protocol conformance by checking the various count and length fields for consistency.
Enhanced H.323 Inspection	This feature allows you to change the default configuration values used for H.323 application inspection. H.323 inspection supports RAS, H.225, and H.245, and its functionality translates all embedded IP addresses and ports. It performs state tracking and filtering and can do a cascade of inspect function activation. H.323 inspection supports phone number filtering, dynamic T.120 control, H.245 tunneling control, protocol state tracking, H.323 call duration enforcement, and audio and video control.
Enhanced DNS Inspection	This feature allows you to specify actions when a message violates a parameter that uses a DNS inspection policy map. DNS application inspection supports DNS message controls that provide protection against DNS spoofing and cache poisoning. User configurable rules allow filtering based on the DNS header, domain name, and resource record TYPE and CLASS.
Enhanced FTP Inspection	This feature allows you to change the default configuration values used for FTP application inspection. FTP command filtering and security checks are provided using strict FTP inspection for improved security and control. Protocol conformance includes packet length checks, delimiters and packet format checks, command terminator checks, and command validation. Blocking FTP based on user values is also supported so that it is possible for FTP sites to post files for download but restrict access to certain users. You can block FTP connections based on file type, server name, and other attributes. System message logs are generated if an FTP connection is denied after inspection.
Enhanced HTTP Inspection	This feature allows you to change the default configuration values used for HTTP application inspection. HTTP application inspection scans HTTP headers and body and performs various checks on the data. These checks prevent various HTTP constructs, content types, and tunneling and messaging protocols from traversing the security appliance. HTTP application inspection can block tunneled applications and non-ASCII characters in HTTP requests and responses, preventing malicious content from reaching the web server. Size limiting of various elements in HTTP request and response headers, URL blocking, and HTTP server header type spoofing are also supported.

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
Enhanced Skinny (SCCP) Inspection	This feature allows you to change the default configuration values used for SCCP (Skinny) application inspection. Skinny application inspection performs translation of embedded IP address and port numbers within the packet data and dynamic opening of pinholes. It also performs additional protocol conformance checks and basic state tracking.
Enhanced SIP Inspection	This feature allows you to change the default configuration values used for SIP application inspection. SIP is a widely used protocol for Internet conferencing, telephony, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats. SIP application inspection provides address translation in the message header and body, dynamic opening of ports, and basic sanity checks. It also supports application security and protocol conformance, which enforces the sanity of the SIP messages, as well as detects SIP-based attacks.
Instant Messaging (IM) Inspection	This feature allows you to change the default configuration values used for Instant Messaging (IM) application inspection. Instant Messaging (IM) application inspection provides detailed access control to control network usage. It also helps stop leakage of confidential data and propagations of network threats. A regular expression database search that represents various patterns for Instant Messaging (IM) protocols to be filtered is applied. A syslog is generated if the flow is not recognized. The scope can be limited by using an access list to specify any traffic streams to be inspected. For UDP messages, a corresponding UDP port number is also configurable. Inspection of Yahoo! Messenger and MSN Messenger instant messages are supported.
MPF-Based Regular Expression Classification Map	This feature allows you to define regular expressions in Modular Policy Framework class maps and match a group of regular expressions that has the **match-any** attribute. You can use a regular expression class map to match the content of certain traffic; for example, you can match URL strings inside HTTP packets.
Radius Accounting Inspection	This feature allows you to protect against an over-billing attack in the Mobile Billing Infrastructure. The **policy-map type inspect radius-accounting** command was introduced in this version.
GKRCS Support for H.323	Two control signaling methods are described in the ITU-T H.323 recommendation: Gatekeeper Routed Control Signaling (GKRCS) and Direct Call Signalling (DCS). DCS is supported by the Cisco IOS gatekeeper. This feature adds Gatekeeper Routed Control Signaling (GKRCS) control signaling method support.
Skinny Video Support	This feature adds SCCP version 4.1.2 message support to print the message name processed by the inspect feature when **debug skinny** is enabled. CCM 4.0.1 messages are supported.

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
SIP IP Address Privacy	This feature allows you to retain the outside IP addresses embedded in inbound SIP packets for all transactions, except REGISTER (because it is exchanged between the proxy and the phone), to hide the real IP address of the phone. The REGISTER message and the response to REGISTER message will be exempt from this operation because this message is exchanged between the phone and the proxy. When this feature is enabled, the outside IP addresses in the SIP header and SDP data of inbound SIP packets will be retained. Use the **ip-address-privacy** command to turn on this feature.
RTP/RTCP Inspection	This feature NATs embedded IP addresses and opens pinholes for RTP and RTCP traffic. This feature ensures that only RTP packets flow on the pinholes opened by Inspects SIP, Skinny, and H.323. To prevent a malicious application from sending UDP traffic to make use of the pinholes created on the security appliance, this feature allows you to monitor RTP and RTCP traffic and to enforce the validity of RTP and RTCP packets.
Remote Access and Site-to-Site VPN Features	

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
Network Admission Control	Network Admission Control (NAC) allows you to validate a peer based on its state. This method is referred to as posture validation (PV). PV can include verifying that the peer is running applications with the latest patches, and ensuring that the antivirus files, personal firewall rules, or intrusion protection software that runs on the remote host are up to date. An Access Control Server (ACS) must be configured for Network Admission Control before you configure NAC on the security appliance. As a NAC authenticator, the security appliance does the following: • Initiates the initial exchange of credentials based on IPsec session establishment and periodic exchanges thereafter. • Relays credential requests and responses between the peer and the ACS. • Enforces the network access policy for an IPsec session based on results from the ACS server. • Supports a local exception list based on the peer operating system, and optionally, an ACL. • (Optional) Requests access policies from the ACS server for a clientless host. As an ACS client, the security appliance supports the following: • EAP/RADIUS • RADIUS attributes required for NAC NAC on the security appliance differs from NAC on Cisco IOS Layer 3 devices (such as routers) where routers trigger PV based on routed traffic. The security appliance enabled with NAC uses an IPsec VPN session as the trigger for PV. Cisco IOS routers configured with NAC use an Intercept ACL to trigger PV based on traffic destined for certain networks. Because external devices cannot access the network behind the security appliance without starting a VPN session, the security appliance does not need an intercept ACL as a PV trigger. During PV, all IPsec traffic from the peer is subject to the default ACL configured for the peer's group. Unlike the Cisco VPN 3000 Concentrator Series, NAC on the security appliance supports stateless failover, initialization of all NAC sessions in a tunnel group, revalidation of all NAC sessions in a tunnel group, and posture validation exemption lists configured for each tunnel group. NAC on the security appliance does not support non-VPN traffic, IPv6, security contexts, and WebVPN. By default, NAC is disabled. You can enable it on a group policy basis.

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
L2TP Over IPsec	Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clients to use the public IP network to communicate securely with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data. L2TP is based on the client/server model. The function is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator (LAC). The LNS typically runs on a network gateway such as a router, while the LAC can be a dial-up Network Access Server (NAS), or a PC with a bundled L2TP client such as Microsoft Windows 2000. L2TP/IPsec provides the capability to deploy and administer an L2TP VPN solution alongside the IPsec VPN and firewall services in a single platform. The primary benefit of configuring L2TP with IPsec in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, enabling remote access from virtually anyplace with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN). No additional client software, such as Cisco VPN client software, is required.
OCSP Support	The Online Certificate Status Protocol (OCSP) provides an alternative to CRL for obtaining the revocation status of X.509 digital certificates. Rather than requiring a client to download a complete and often large certificate revocation list, OCSP localizes the certificate status on a Validation Authority, which it queries for the status of a specific certificate.
Multiple L2TP Over IPsec Clients Behind NAT	The security appliance can successfully establish remote-access L2TP-over-IPsec connections to more than one client behind one or more NAT devices. This enhances the reliability of L2TP over IPsec connections in typical SOHO/branch office environment environments, where multiple L2TP over IPsec clients must communicate securely with a central office.
Nokia Mobile Authentication Support	You can establish a VPN using a handheld Nokia 92xx Communicator series cellular device for remote access. The authentication protocol that these devices use is the IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) protocol.
Zonelabs Integrity Server	You can configure the security appliance in a network that deploys the Zone Labs Integrity System to enforce security policies on remote VPN clients. In this case, the security appliance is an edge gateway between the Zone Labs Integrity server and the remote clients. The Zone Labs Integrity server and the Zone Labs Personal Firewall on the remote client ensure that a remote client complies with a centrally managed security policy before the client can access private network resources. You configure the security appliance to pass security policy information between the server and clients to maintain or close client connections to prevent a server connection failure, and to optionally, require SSL certificate authentication of both the Integrity server and the security appliance.
Hybrid XAUTH	You can configure hybrid authentication to enhance the IKE security between the security appliance and remote users. With this feature, IKE Phase I requires two steps. The security appliance first authenticates to the remote VPN user with standard public key techniques and establishes an IKE security association that is unidirectionally authenticated. An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use any one of the supported authentication methods. Hybrid XAUTH allows you to use digital certificates for security appliance authentication and a different method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID.
IPsec Fragmentation and Reassembly Statistics	You can monitor additional IPsec fragmentation and reassembly statistics that help to debug IPsec-related fragmentation and reassembly issues. The new statistics provide information about fragmentation and reassembly both before and after IPsec processing.

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
Inspection IPS, CSC and URL Filtering for WebVPN	This feature adds support for inspection, IPS, and Trend Micro for WebVPN traffic in clientless mode and port forwarding mode. Support for SVC mode is preexisting. In all of the modes, the Trend Micro and the IPS engines will be triggered (if configured). URL/FTP/HTTPS/Java/Activex filtering using WebSense and N2H2 support has also been added. DNS inspect will be triggered for the DNS requests. In port forwarding mode, HTTP, SMTP, FTP, and DNS inspections with the filtering mechanisms using WebSense and N2H2 support has been added.
Routing Features	
Active RIP Support	The security appliance supports RIP Version 1 and RIP Version 2. You can only enable one RIP routing process on the security appliance. When you enable the RIP routing process, RIP is enabled on all interfaces. By default, the security appliance sends RIP Version 1 updates and accepts RIP Version 1 and Version 2 updates. To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode.
Standby ISP Support	This feature allows you to configure a link standby ISP if the link to your primary ISP fails. It uses static routing and object tracking to determine the availability of the primary route and to activate the secondary route when the primary route fails.
PPPoE Client	Point-to-Point Protocol over Ethernet (PPPoE) combines two widely accepted standards, Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. PPPoE clients are typically personal computers connected to an ISP over a remote broadband connection, such as DSL or cable service. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use.
Dynamic DNS Support	You can create dynamic DNS (DDNS) update methods and configure them to update the Resource Records (RRs) on the DNS server at whatever frequency you need. DDNS complements DHCP, which enables users to dynamically and transparently assign reusable IP addresses to clients. DDNS then provides dynamic updating and synchronizing of the name to the address and the address to the name mappings on the DNS server. With this version, the security appliance supports the IETF standard for DNS record updates.
Multicast Routing Enhancements	Multicast routing enhancements allows you to define multicast boundaries so that domains with RPs that have the same IP address do not leak into each other, to filter PIM neighbors to better control the PIM process, and to filter PIM bidir neighbors to support mixed bidirectional and sparse-mode networks.
Expanded DNS Domain Name Usage	You can use DNS domain names, such as www.example.com, when configuring AAA servers and also with the **ping**, **traceroute**, and **copy** commands.
Intra-Interface Communication for Clear Traffic	You can now allow any traffic to enter and exit the same interface, and not just VPN traffic.
IPv6 Security Enforcement of IPv6 Addresses	This feature allows you to configure the security appliance to require that IPv6 addresses for directly connected hosts use the Modified EUI-64 format for the interface identifier portion of the address.
Multiple Context Mode Features	

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
Private and Automatic MAC Address Assignments and Generation for Multiple Context Mode	You can assign a private MAC address (both active and standby for failover) for each interface. For multiple context mode, you can automatically generate unique MAC addresses for shared context interfaces, which makes classifying packets into contexts more reliable. The new **mac-address auto** command allows you to automatically assign private MAC addresses to each shared context interface.
Resource Management for Security Contexts	If you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.
Save All Context Configurations from the System	You can now save all context configurations at once from the system execution space using the **write memory all** command.
High Availability Features	
Sub-second Failover	This feature allows you to configure failover to detect and respond to failures in under a second.
Configurable Prompt	With this feature, the user can see the failover status of the security appliance without having to enter the **show failover** command and parse the output. This feature allows users to see the chassis slot number of the failover unit. Previously, the prompt reflected just the hostname, security context, and configuration mode. The **prompt** command provides support for this feature.
Firewall Features	
Generic Input Rate Limiting	This feature prevents denial of service (DoS) attacks on a security appliance or on certain inspection engines on a firewall. The 7.0 release supports egress rate-limiting (police) functionality and in this release, input rate-limiting functionality extends the current egress policing functionality. The **police** command is extended for this functionality.
Authentication for Through Traffic and Management Access Supports All Servers Previously Supported for VPN Clients	All server types can be used for firewall authentication with the following exceptions: HTTP Form protocol supports single sign-on authentication for WebVPN users only and SDI is not supported for HTTP administrative access.
Dead Connection Detection (DCD)	This feature allows the adaptive security appliance to automatically detect and expire dead connections. In previous versions, dead connections never timed out; they were given an infinite timeout. Manual intervention was required to ensure that the number of dead connections did not overwhelm the security appliance. With this feature, dead connections are detected and expired automatically, without interfering with connections that can still handle traffic. The set connection timeout and show service-policy commands provide DCD support.
WCCP	The Web Cache Communication Protocol (WCCP) feature allows you to specify WCCP service groups and redirect web cache traffic. The feature transparently redirects selected types of traffic to a group of web cache engines to optimize resource usage and lower response times.
Filtering Features	
URL Filtering Enhancements for Secure Computing (N2H2)	This feature allows you to enable long URL, HTTPS, and FTP filtering by using both Websense (the current vendor) and N2H2 (a vendor that has been purchased by Secure Computing). Previously, the code only enabled the vendor Websense to provide this type of filtering. The url-block, url-server, and filter commands provide support for this feature.
Management and Troubleshooting Features	

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
Auto Update	The security appliance can now be configured as an Auto Update server in addition to being configured as an Auto Update client. The existing **client-update** command (which is also used to update VPN clients) is enhanced to support the new Auto Update server functionality, and includes new keywords and arguments that the security appliance needs to update security appliances configured as clients. For the security appliance configured as an Auto Update client, the auto-update command continues to be the command used to configure the parameters that the security appliance needs to communicate with the Auto Update server.
Modular Policy Framework Support for Management Traffic	You can now define a Layer 3/4 class map for to-the-security-appliance traffic, so you can perform special actions on management traffic. For this version, you can inspect RADIUS accounting traffic.
Traceroute	The **traceroute** command allows you to trace the route of a packet to its destination.
Packet Tracer	The packet tracer tool allows you to trace the life span of a packet through the security appliance to see if it is behaving as expected. The new patent-pending Packet Tracer tool in ASDM lets you easily trace the life span of a packet through the security appliance in an animated packet flow model to see if it is behaving as expected and simplify troubleshooting no matter how complex the network design. The tool provides the attributes of a packet such as source and destination IP addresses with a visual representation of the different phases of the packet and the relevant configuration, which is accessible with a single click. For each phase, it displays whether the packet is dropped or allowed.
ASDM Features	
Enhanced ASDM rules table	The ASDM rule tables have been redesigned to streamline policy creation. In addition to simplified rule creation that maps more closely with CLI, the rule tables support most configuration scenarios including super-netting and using an object group that is associated to more than interface. The use of ASDM location and ASDM group was removed to simplify the creation of rules. You now have the ability to: • Create objects, object-groups and rules from a single panel • Filter on interfaces, source, destination or services • Policy query in the rule tbale for advanced filtering using multiple conditions • Show logs for a particular access rule in the real time log viewer • Select a rule and packet trace with a single click which will populate with appropriate packet attributes • Easily organize and move up and down in the table to change the order of access list entries • Expand and display elements in an object group • See attributes of a object or memebers of a group via tooltips
High Availability and Scalability Wizard	The High Availability and Scalability Wizard is used to simplify configuration of Active/Active, Active/Standy failover and VPN Load balancing. The wizard also intelligently configures the peer device.

Table 1 New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)

Feature	Description
Syslog enhancements	Enhancements to the syslog features include: • Syslog parsing to display source IP, destination IP, syslog ID, date and time into different columns • Integrated syslog references with explanations and recommended actionss for each syslog with a single click • Syslog coloring based on severity level • A brief explanation of the syslogs as a tool tip in the log viewer
NAT rules	The creation of NAT rules is simplified.
Object group support	There is now full ASDM support of network, service, protocol and ICMP-type object groups.
Named IP addresses	The ability to create a name to be associated with an IP Address now exists.
ASDM Assistant	The new ASDM Assistant provides task-oriented guidance to configuring features such as AAA server, logging filters, SSL VPN Client, and others features. You can also upload new guides.
Context management	Context management is improved, including context caching and better scalability.
Inspection maps	Predefined low, medium and high security settings simplify creation and management of inspection maps.

Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for Version 5.2(1).

Table 2 Operating System and Browser Requirements

	Operating System	Browser	Other Requirements
Windows[1]	Windows 2000 (Service Pack 4) or Windows XP operating systems (English or Japanese versions)	Internet Explorer 6.0 with Sun Java[2] Plug-in 1.4.2 or 5.0 (1.5.0) -or- Firefox 1.5 with Java Plug-in 1.4.2 or 5.0 (1.5.0) **Note** **HTTP 1.1**—Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections.	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Sun Solaris	Sun Solaris 8 or 9 running CDE window manager	Mozilla 1.7.3 with Sun Java Plug-in 1.4.2 or 1.5.0	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 3 running GNOME or KDE	Firefox 1.5 with Java Plug-in 1.4.2 or 5.0 (1.5.0)[3]	

1. ASDM is not supported on Windows 3.1, 95, 98, ME or Windows NT4.

2. Get Sun Java from java.sun.com.
3. On Windows and Linux, Firefox 1.5 replaces Mozilla 1.7.3, which was used in previous ASDM releases.

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 and Solaris

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 Close all instances of Internet Explorer or Netscape.

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 and Solaris

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

Step 1 Close all instances of Netscape or Mozilla.

Step 2 Bring up Java Plug-in Control Panel by launching the ControlPanel executable file.

Note In the Java 2 SDK, this file is located in *SDK installation directory*/jre/bin/ControlPanel. For example if your 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		

Table 3 ASA 5505 Adaptive Security Appliance License Features (continued)

ASA 5505	Base License		Security Plus	
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)		5 (3 zones, 1 failover link, and 1 backup ISP link)	
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	128 MB		128 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*		*10*	*25*	*50*	*100*	*250*
VPN Load Balancing	No support					No support					
Failover	None					Active/Standby or Active/Active					
GTP/GPRS	No support					No support					
Max. VLANs	10					25					
Concurrent Firewall Conns[2]	50 K					130 K					
Max. Physical Interfaces	3 at 10/100 plus the Management interface for management traffic only					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						
Max. WebVPN Sessions	2	*Optional Licenses:*					
		10	*25*	*50*	*100*	250	*500*	*750*
VPN Load Balancing	Supported						
Failover	Active/Standby or Active/Active						
GTP/GPRS	None	*Optional license: Enabled*					
Max. VLANs	100						
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								
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								

Table 6 ASA 5540 Adaptive Security Appliance License Features (continued)

ASA 5540	Base License	
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									
Failover	Active/Standby or Active/Active									
GTP/GPRS	None	*Optional license: Enabled*								
Max. VLANs	200									
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

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]		
VPN Load Balancing	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	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
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*
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			
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

For a table showing ASDM compatibility with SSMs, see:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

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:

- In ASDM 5.0 and 5.1, click **Upload Image from Local PC**.
- In ASDM 5.2, click **Upgrade Software**.

Step 4 With ASDM selected, click the **Browse Local** button 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 the **Browse Flash** button.

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, you see the following message:

"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 quit out of 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 SSM (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 login 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 it back to the original configuration.
  - 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:

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 Click the **Run in Demo Mode** check box.

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

Step 5 If you want 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 your security appliance:

Step 1 Launch the wizard according to the steps for your 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 your configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of your connection changes.

Step 4 You can now 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:

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 the **Help** button for more information on each field.

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

Configuring Stateful Failover

This section describes how to implement Stateful Failover on security appliances connected via a LAN.

If you are connecting two adaptive security appliances for failover, you must connect them via a LAN. If you are connecting two security appliances, you can connect them using either a LAN or a serial cable.

Tip If your security appliances are located near each other, you might prefer connecting them with a serial cable to connecting them via the LAN. Although the serial cable is slower than a LAN connection, using a cable prevents having to use an interface or having the LAN and Stateful Failover share an interface, which could affect performance. Also, using a cable enables the detection of power failure on the peer device.

As specified in the *Cisco Security Appliance Command Line Configuration Guide,* both devices must have appropriate licenses and have the same hardware configuration.

Before you begin, decide on active and standby IP addresses for the interfaces ASDM connects through on the primary and secondary devices. These IP addresses must be assigned to device interfaces with HTTPS access.

To configure LAN Stateful Failover on your security appliance, perform the following steps:

Step 1 Configure the secondary device for HTTPS IP connectivity. See the Before You Begin, page 21, and use a different IP address on the same network as the primary device.

Step 2 Connect the pair of devices together and to their networks in their Stateful Failover LAN cable configuration.

Step 3 Start ASDM from the primary device through a supported web browser. (See the section Downloading the ASDM Launcher, page 22.)

Step 4 Perform one of the following steps, depending on your context mode:

a. If your device is in multiple context mode, click **Context**. Choose the **admin** context from the **Context** drop-down menu, and click **Configuration > Properties > Failover**.

b. If your device is in single mode, click **Configuration > Properties > Failover**. Click the **Interfaces** tab.

Step 5 Perform one of the following steps, depending on your firewall mode:

a. If your device is in routed mode, configure standby addresses for all routed mode interfaces.

b. If your device is in transparent mode, configure a standby management IP address.

Note Interfaces used for failover connectivity should not have names (in single mode) or be allocated to security contexts (in multiple security context mode). In multiple context mode, other security contexts may also have standby IP addresses configured.

Step 6 Perform one of the following steps, depending on your security context mode:

a. If your device is in multiple security context mode: click **System > Configuration > Failover**.

b. If your device is in single mode: click **Configuration > Properties > Failover**.

Step 7 On the **Setup** tab of the **Failover** pane under **LAN Failover**, select the interface that is cabled for LAN Stateful Failover.

Step 8 Configure the remaining **LAN Failover** fields.

Step 9 (Optional) Provide information for other fields in all of the failover tabs. If you are configuring Active/Active failover, you must configure failover groups in multiple security context mode. If more than one failover pair of devices coexist on a LAN in Active/Active Stateful Failover, provide failover-group MAC addresses for any interfaces on shared LAN networks.

Step 10 On the **Setup** tab, check the **Enable Failover** check box. If you are using the PIX 500 series security appliance, check the **Enable LAN rather than serial cable failover** check box.

Step 11 Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.

Step 12 Enter the IP address of the secondary device, which you configured as the standby IP address of the ASDM interface. Wait about 60 seconds. The standby peer still could become temporarily inaccessible.

Step 13 Click **OK**. Wait for configuration to be synchronized to the standby device over the failover LAN connection.

The secondary device should now enter standby failover state using the standby IP addresses. Any further configuration of the active device or an active context is replicated to the standby device or the corresponding standby context.

Securing the Failover Key

To prevent the failover key from being replicated to the peer unit in clear text for an existing failover configuration, disable failover on the active unit (or in the system execution space on the unit that has failover group 1 in the active state), enter the failover key on both units, and then reenable failover. When Stateful Failover is reenabled, the failover communication is encrypted with the key.

To secure the failover key, follow this procedure on the active device:

Step 1 Perform one of the following steps, depending on your security context mode:

a. If your device is in single mode, navigate to **Configuration > Properties > Failover > Setup**.

b. If you device is in multiple mode, navigate to **System > Configuration> Failover > Setup**.

Step 2 Turn off failover. (The standby should switch to pseudo-standby mode.)

a. Uncheck the **Enable failover** check box.

b. Click **Apply**. (Click **OK** if CLI preview is enabled.)

Step 3 Enter the failover key in the **Shared Key** box.

Step 4 Reenable failover.

a. Check the **Enable failover** check box.

b. Click **Apply**. (Click **OK** if CLI preview is enabled.) A dialog box about configuring the peer appears.

Step 5 Enter the IP address of the peer. Wait about 60 seconds. Even though the standby peer does not have the shared failover key, the standby peer still could become inaccessible.

Step 6 Click **OK**. (Click **OK** if CLI preview is enabled.) Wait for configuration to be synchronized to the standby device over the encrypted failover LAN connection.

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 which 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 sections:

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, see **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 3 by your system administrator, which allows Monitor-only mode. For more information, see **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 added by the CLI, but that cannot be added or edited in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If it is view-only, then the command 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
failover timeout	Ignored
ipv6, any IPv6 addresses	Ignored
pager	Ignored
pim accept-register route-map	Ignored. Only the **list** option can be configured 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 panels.
- For CLI commands that have a noconfirm option, use the noconfirm 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 language other than English, be careful not to enter non-English characters accidentally.

Workaround:

For workarounds, see CSCeh39437 under Caveats, page 31.

Caveats

The following sections describe caveats for the 5.2(1) release.

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/

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

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

Open Caveats - Release 5.2(1)

Table 11 Open Caveats

	Software Release 5.2(1)	
ID Number	Corrected	Caveat Title
CSCse15764	No	ASDM: File > Print very slow to execute
CSCse27211	No	When you modify an ACE for remark or logging, ASDM issues clear xlate
CSCse27112	No	QoS Help: SgzApplet-0: Httpd: no such entry help/mappingfiles/csdm_hlp.j
CSCse27696	No	Negating a regex range [] give a false warning message
CSCse30178	No	interface cost does not sort correctly
CSCse07045	No	Service policy classes not listed in same order as the CLI
CSCsd75599	No	Modifying a shared extended ACL should warn user of sharing implications
CSCse12224	No	MGCP: all panels help not present, or not correct or shows wrong window
CSCse25002	No	HAS wizard doesn't catch same active/standby IP for fail and state links
CSCse02013	No	Cannot delete failover group 2 if it is in the first row of the table
CSCse23663	No	Status window and command preview window pop up at same time on Linux
CSCsd93317	No	Some multicast commands are not supported by ASDM
CSCse27211	No	When you modify an ACE for remark or logging, ASDM issues "clear xlate”
CSCse27696	No	Negating a regex range [] give a false warning message
CSCse32907	No	ASDM: 'Delete All APCF Profiles' cannot be executed- Apply grayed
CSCse33050	No	Unnamed interfaces not listed in backup interface drop down
CSCse33796	No	VPN Monitoring Sessions:Peer IP not filled in when using VPN Server
CSCse33814	No	SIP map: if log only action configured, won't show for some field cm
CSCse33948	No	Startup Wizard does not recognize or save PPPoE IP address setting
CSCse34030	No	ASDM incorrectly allows configuring ASA 5505 to boot from a TFTP server
CSCse34044	No	Startup Wizard cannot configure or read static route monitoring option
CSCse35076	No	"WebVPN Auto Signon" tab in user/Group should be grayed out

Table 11 Open Caveats (continued)

	Software Release 5.2(1)	
ID Number	Corrected	Caveat Title
CSCse35606	No	Log viewer Show Rule doesn't return to Access Rules table
CSCse38580	No	IPSec Rules: PFS configuration problems
CSCse38624	No	The Home Page display is not completely shown in some situations

Resolved Caveats - Release 5.2(1)

The following list shows caveats that are resolved for Version 5.2(1):

Table 12 Resolved Caveats

	Software Release 5.2(1)	
ID Number	Corrected	Caveat Title
CSCsd26144	Yes	Trustpoint enrollment URL field - missing validation
CSCsd26151	Yes	Generating default key-pair gives an error
CSCsd26163	Yes	CLI tool: not clear that the command drop-down is editable
CSCsd26165	Yes	VPN Wizard, Site-to-Site: remote peer tunnel group name can't be changed
CSCsd82585	Yes	Making change to AAA server results in no-change
CSCsd96769	Yes	Edit Rule Query does not show Field value

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 Quick Start Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco PIX Security Appliance Release Notes*
- *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.

OThis document is to be used in conjunction with the documents listed in the "Obtaining Documentation and Submitting a Service Request" section.