CHAPTER 1

Introduction to the Security Appliance

The security appliance combines advanced stateful firewall and VPN concentrator functionality in one device, and for some models, an integrated intrusion prevention module called the AIP SSM or an integrated content security and control module called the CSC SSM. The security appliance includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPSec and clientless SSL support, and many more features. See the "Supported Feature Licenses Per Model" section on page 3-1 for a list of supported platforms and features. For a list of new features, see the *Cisco ASA 5500 Series Release Notes* or the *Cisco PIX Security Appliance Release Notes*.

This chapter includes the following sections:

Supported Platform Models

Software Version 8.0 is supported on the following platform models:

- ASA 5505
- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- PIX 515/515E
- PIX 525
- PIX 535

Note The Cisco PIX 501 and PIX 506E security appliances are not supported in any version; all other PIX models are supported in Version 8.0(4) and earlier only.

The ASA 5580 is not supported in Version 8.0.

For information about licenses and features supported on each platform, see Chapter 3, "Managing Feature Licenses."

SSM and SSC Support Per Model

Table 1-1 shows the SSMs supported by each platform:

Table 1-1 SSM Support

Platform	SSM Models
ASA 5505	No support
ASA 5510	AIP SSM 10 AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5520	AIP SSM 10 AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5540	AIP SSM 10 AIP SSM 20 CSC SSM 10[1] CSC SSM 20[1] 4GE SSM
ASA 5550	No support (the 4GE SSM is built-in and not user-removable)

1. The CSC SSM licenses support up to 1000 users while the Cisco ASA 5540 Series appliance can support significantly more users. If you deploy CSC SSM with an ASA 5540 adaptive security appliance, be sure to configure the security appliance to send the CSC SSM only the traffic that should be scanned.

VPN Specifications

See the *Cisco ASA 5500 Series VPN Compatibility Reference* at
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

New Features

This section lists the features added for each maintenance release, and includes the following topics:

New Features in Version 8.0(5)

Released: November 3, 2009

Table 1-2 lists the new features forASA Version 8.0(5).

Note Version 8.0(5) is not supported on the PIX security appliance.

Table 1-2 New Features for ASA Version 8.0(5)

Feature	Description
Remote Access Features	
Scalable Solutions for Waiting-to-Resume VPN Sessions	An administrator can now keep track of the number of users in the active state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in *Also available in Version 8.2(2).*
Application Inspection Features	
Enabling Call Set up Between H.323 Endpoints	You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The security appliance includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the security appliance opens a pinhole through source IP address/port 0/0. By default, this option is disabled. The following command was introduced:**ras-rcf-pinholes enable**. Use this command during parameter configuration mode while creating an H.323 Inspection policy map. *Also available in Version 8.2(2).*
Interface Features	

Table 1-2 New Features for ASA Version 8.0(5) (continued)

Feature	Description
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresess are also now persistent accross reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2. The following command was modified: **mac-address auto prefix** *prefix*. *Also available in Version 8.2(2).*
High Availablility Features	
No notifications when interfaces are brought up or brought down during a switchover event	To distinguish between link up/down transitions during normal operation from link up/down transitions during failover, no link up/link down traps are sent during a failover. Also, no syslog messages about link up/down transitions during failover are sent. *Also available in Version 8.2(2).*
Routing Features	
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	This enhancement introduces security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each DHCP server that is configured using the **dhcp-server** command, you can now configure the security appliance to send the **subnet-selection** option, and the **link-selection** option or neither. *Also available in Version 8.2(2).*

New Features in Version 8.0(4)

Released: August 11, 2008

Table 1-3 lists the new features forASA or PIX Version 8.0(4).

Table 1-3 New Features for ASA and PIX Version 8.0(4)

Feature	Description
Unified Communications Features[1]	
Phone Proxy	Phone Proxy functionality is supported. ASA Phone Proxy provides similar features to those of the Metreos Cisco Unified Phone Proxy with additional support for SIP inspection and enhanced security. The ASA Phone Proxy has the following key features: • Secures remote IP phones by forcing the phones to encrypt signaling and media • Performs certificate-based authentication with remote IP phones • Terminates TLS signaling from IP phones and initiates TCP and TLS to Cisco Unified Mobility Advantage servers • Terminates SRTP and initiates RTP/SRTP to the called party

Table 1-3 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
Mobility Proxy	Secure connectivity (mobility proxy) between Cisco Unified Mobility Advantage clients and servers is supported. Cisco Unified Mobility Advantage solutions include the Cisco Unified Mobile Communicator, an easy-to-use software application for mobile handsets that extends enterprise communications applications and services to mobile phones and smart phones and the Cisco Unified Mobility Advantage server. The mobility solution streamlines the communication experience, enabling real-time collaboration across the enterprise. The ASA in this solution delivers inspection for the MMP (formerly called OLWP) protocol, the proprietary protocol between Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage. The ASA also acts as a TLS proxy, terminating and reoriginating the TLS signaling between the Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage.
Presence Federation Proxy	Secure connectivity (presence federation proxy) between Cisco Unified Presence servers and Cisco/Microsoft Presence servers is supported. With the Presence solution, businesses can securely connect their Cisco Unified Presence clients back to their enterprise networks, or share Presence information between Presence servers in different enterprises. The ASA delivers functionality to enable Presence for Internet and intra-enterprise communications. An SSL-enabled Cisco Unified Presence client can establish an SSL connection to the Presence Server. The ASA enables SSL connectivity between server to server communication including third-party Presence servers communicating with Cisco Unified Presence servers. Enterprises share Presence information, and can use IM applications. The ASA inspects SIP messages between the servers.
Remote Access Features	
Auto Sign-On with Smart Tunnels for IE[1]	This feature lets you enable the replacement of logon credentials for WININET connections. Most Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does not, so it is not supported by this feature. It also supports HTTP-based authentication, therefore form-based authentication does not work with this feature. Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. Also, because of the association with destinations hosts, providing support for an auto sign-on enabled host may not be desirable if you want to deny access to some of the services on that host. To configure a group auto sign-on for smart tunnels, you create a global list of auto sign-on sites, then assign the list to group policies or user names. This feature is not supported with Dynamic Access Policy.
Entrust Certificate Provisioning[1]	ASDM includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA.

Table 1-3 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
Extended Time for User Reauthentication on IKE Rekey	You can configure the security appliance to give remote users more time to enter their credentials on a Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunnels and a phase 1 rekey occurred, the security appliance prompted the user to authenticate and only gave the user approximately 2 minutes to enter their credentials. If the user did not enter their credentials in that 2 minute window, the tunnel would be terminated. With this new feature enabled, users now have more time to enter credentials before the tunnel drops. The total amount of time is the difference between the new Phase 1 SA being established, when the rekey actually takes place, and the old Phase 1 SA expiring. With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the rekey interval.
Persistent IPsec Tunneled Flows	With the persistent IPsec tunneled flows feature enabled, the security appliance preserves and resumes stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dropped when the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP flows allows some older or sensitive applications to keep working through a short-lived tunnel drop. This feature supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a Hardware Client. It does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the **[no] sysopt connection preserve-vpn-flows** command. This option is disabled by default.
Show Active Directory Groups	The CLI command **show ad-groups** was added to list the active directory groups. ASDM Dynamic Access Policy uses this command to present the administrator with a list of MS AD groups that can be used to define the VPN policy.
Smart Tunnel over Mac OS[1]	Smart tunnels now support Mac OS.
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in use is not being eliminated from the pool, the connection is not affected. However, if the address in use is being eliminated from the pool, the connection is brought down. *Also available in Version 7.0(8) and 7.2(4).*
Firewall Features	
QoS Traffic Shaping	If you have a device that transmits packets at a high speed, such as the security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the **shape** command. See also the **crypto ipsec security-association replay** command, which lets you configure the IPSec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPSec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms. *Also available in Version 7.2(4).*

Table 1-3 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
TCP Normalization Enhancements	You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets. • TCP invalid ACK check (the **invalid-ack** command) • TCP packet sequence past window check (the **seq-past-window** command) • TCP SYN-ACK with data check (the **synack-data** command) You can also set the TCP out-of-order packet buffer timeout (the **queue** command **timeout** keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value. The default action for packets that exceed MSS has changed from drop to allow (the **exceed-mss** command). The following non-configurable actions have changed from drop to clear for these packet types: • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option *Also available in Version 7.2(4).*
TCP Intercept statistics	You can enable collection for TCP Intercept statistics using the **threat-detection statistics tcp-intercept** command, and view them using the **show threat-detection statistics** command.
Threat detection shun timeout	You can now configure the shun timeout for threat detection using the **threat-detection scanning-threat shun duration** command.
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the **timeout sip-provisional-media** command. *Also available in Version 7.2(4).*
clear conn Command	The **clear conn** command was added to remove connections. *Also available in Version 7.0(8) and 7.2(4).*
Fragment full reassembly	The **fragment** command was enhanced with the **reassembly full** keywords to enable full reassembly for fragments that are routed through the device. Fragments that terminate at the device are always fully reassembled. *Also available in Version 7.0(8) and 7.2(4).*
Ethertype ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules are retained, but no new ones need to be added. *Also available in Version 7.0(8) and 7.2(4).*
Troubleshooting and Monitoring Features	
capture command Enhancement	The **capture type asp-drop** *drop_code* command now accepts **all** as the *drop_code*, so you can now capture all packets that the security appliance drops, including those dropped due to security checks. *Also available in Version 7.0(8) and 7.2(4).*

Table 1-3 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
show asp drop Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the drop reason keywords next to the description, so you can easily use the **capture asp-drop** command using the keyword. *Also available in Version 7.0(8) and 8.0(4).*
clear asp table Command	Added the **clear asp table** command to clear the hits output by the **show asp table** commands. *Also available in Version 7.0(8) and 7.2(4).*
show asp table classify hits Command Enhancement	The **hits** option was added to the **show asp table classify** command, showing the timestamp indicating the last time the asp table counters were cleared. It also shows rules with hits values not equal to zero. This permits users to quickly see what rules are being hit, especially since a simple configuration may end up with hundreds of entries in the **show asp table classify** command. *Also available in Version 7.0(8) and 8.0(4).*
MIB Enhancement	The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely. *Also available in 8.0(4).*
show perfmon Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Attempts, TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept. *Also available in Version 7.0(8) and 7.2(4).*
memory tracking Commands	The following new commands are introduced in this release: • **memory tracking enable**–This command enables the tracking of heap memory requests. • **no memory tracking enable**–This command disables tracking of heap memory requests, cleans up all currently gathered information, and returns all heap memory used by the tool itself to the system. • **clear memory tracking**–This command clears out all currently gathered information but continues to track further memory requests. • **show memory tracking**–This command shows currently allocated memory tracked by the tool, broken down by the topmost caller function address. • **show memory tracking address**–This command shows currently allocated memory broken down by each individual piece of memory. The output lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool. • **show memory tracking dump**–This command shows the size, location, partial callstack, and a memory dump of the given memory address. • **show memory tracking detail**–This command shows various internal details to be used in gaining insight into the internal behavior of the tool. *Also available in Version 7.0(8) and 7.2(4).*
Routing Features	

Table 1-3 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
IPv6 Multicast Listener Discovery Protocol v2 Support	The security appliance now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to discover the presence of multicast address listeners on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. The security appliance becomes a multicast address listener, or a host, but not a a multicast router, and responds to Multicast Listener Queries and sends Multicast Listener Reports only. The following commands support this feature: • **clear ipv6 mld traffic** The **clear ipv6 mld traffic** command allows you to reset all the Multicast Listener Discovery traffic counters. • **show ipv6 mld traffic** The **show ipv6 mld** command allows you to display all the Multicast Listener Discovery traffic counters. • **debug ipv6 mld** The enhancement to the **debug ipv6** command allows the user to display the debug messages for MLD, to see whether the MLD protocol activities are working properly. • **show debug ipv6 mld** The enhancement to the **show debug ipv6** command allows the user to display whether **debug ipv6 mld** is enabled or disabled. *Also available in Version 7.2(4).*
Platform Features	
Native VLAN support for the ASA 5505	You can now include the native VLAN in an ASA 5505 trunk port using the **switchport trunk native vlan** command. *Also available in Version 7.2(4).*
SNMP support for unnamed interfaces	Previously, SNMP only provided information about interfaces that were configured using the **nameif** command. For example, SNMP only sent traps and performed walks on the IF MIB and IP MIB for interfaces that were named. Because the ASA 5505 has both unnamed switch ports and named VLAN interfaces, SNMP was enhanced to show information about all physical interfaces and logical interfaces; a **nameif** command is no longer required to display the interfaces using SNMP. These changes affect all models, and not just the ASA 5505.
Failover Features	
failover timeout Command	The **failover timeout** command no longer requires a failover license for use with the static nailed feature. *Also available in Version 7.0(8) and 7.2(4).*

1. This feature is not supported on the PIX security appliance.

New Features in Version 8.0(3)

Released: November 7, 2007

Table 1-4 lists the new features forASA and PIX Version 8.0(3).

Table 1-4 New Features for ASA and PIX Version 8.0(3)

Feature	Description
VPN Features	
AnyConnect RSA SoftID API Integration	Provides support for AnyConnect VPN clients to communicate directly with RSA SoftID for obtaining user token codes. It also provides the ability to specify SoftID message support for a connection profile (tunnel group), and the ability to configure SDI messages on the security appliance that match SDI messages received through a RADIUS proxy. This feature ensures the prompts displayed to the remote client user are appropriate for the action required during authentication and the AnyConnect client responds successfully to authentication challenges.
IP Address Reuse Delay	Delays the reuse of an IP address after it has been returned to the IP address pool. Increasing the delay prevents problems the security appliance may experience when an IP address is returned to the pool and reassigned quickly.
Clientless SSL VPN Caching Static Content Enhancement	There are two changes to the clientless SSL VPN caching commands: The **cache-compressed** command is deprecated. The new **cache-static-content** command configures the security appliance to cache all static content, which means all cacheable Web objects that are not subject to SSL VPN rewriting. This includes content such as images and PDF files. The syntax of the command is **cache-static-content** {**enable** | **disable**}. By default, static content caching is disabled. Example: `hostname (config) # webvpn` `hostname (config-webvpn) # cache` `hostname (config-webvpn-cache) # cache-static-content enable` `hostname (config-webvpn-cache) #` *Also available in Version 7.2(3).*
Smart Card Removal Disconnect	This feature allows the central site administrator to configure remote client policy for deleting active tunnels when a Smart Card is removed. The Cisco VPN Remote Access Software clients (both IPSec and SSL) will, by default, tear down existing VPN tunnels when the user removes the Smart Card used for authentication. The following cli command disconnects existing VPN tunnels when a smart card is removed: **smartcard-removal-disconnect** {**enable** | **disable**}. This option is enabled by default. *Also available in Version 7.2(3).*

Table 1-4 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
WebVPN load Balancing	The adaptive security appliance now supports the use of FQDNs for load balancing. To perform WebVPN load balancing using FQDNs, you must enable the use of FQDNs for load balancing, enter the **redirect-fqdn enable** command. Then add an entry for each of your adaptive security appliance outside interfaces into your DNS server if not already present. Each adaptive security appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for reverse lookup. Enable DNS lookups on your adaptive security appliance with the **dns domain-lookup inside** command (or whichever interface has a route to your DNS server). Finally, you must define the ip address, of your DNS server on the adaptive security appliance. Following is the new CLI associated with this enhancement: **redirect-fqdn** {**enable** | **disable**}. *Also available in Version 7.2(3).*
Application Inspection Features	
WAAS and ASA Interoperability	The **inspect waas** command is added to enable WAAS inspection in the policy-map class configuration mode. This CLI is integrated into Modular Policy Framework for maximum flexibility in configuring the feature. The **[no] inspect waas** command can be configured under a default inspection class and under a custom class-map. This inspection service is not enabled by default. The keyword option waas is added to the **show service-policy inspect** command to display WAAS statistics. `show service-policy inspect waas` A new system log message is generated when WAAS optimization is detected on a connection. All L7 inspection services including IPS are bypassed on WAAS optimized connections. System Log Number and Format: %ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection. A new connection flag "W" is added in the WAAS connection. The **show conn detail** command is updated to reflect the new flag. *Also available in Version 7.2(3).*
DNS Guard Enhancement	Added an option to enable or disable DNS guard. When enabled, this feature allows only one DNS response back from a DNS request. *Also available in Version 7.2(3).*

Table 1-4 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
Support for ESMTP over TLS	This enhancement adds the configuration parameter **allow-tls** [**action log**] in the esmtp policy map. By default, this parameter is not enabled. When it is enabled, ESMTP inspection would not mask the 250-STARTTLS echo reply from the server nor the **STARTTLS** command from the client. After the server replies with the 220 reply code, the ESMTP inspection turns off by itself; the ESMTP traffic on that session is no longer inspected. If the **allow-tls action log** parameter is configured, the syslog message ASA-6-108007 is generated when TLS is started on an ESMTP session. `policy-map type inspect esmtp esmtp_map` `parameters` `allow-tls [action log]` A new line for displaying counters associated with the **allow-tls** parameter is added to the **show service-policy inspect esmtp** command. It is only present if **allow-tls** is configured in the policy map. By default, this parameter is not enabled. `show service-policy inspect esmtp` `allow-tls, count 0, log 0` This enhancement adds a new system log message for the **allow-tls** parameter. It indicates on an esmtp session the server has responded with a 220 reply code to the client **STARTTLS** command. The ESMTP inspection engine will no longer inspect the traffic on this connection. System log Number and Format: %ASA-6-108007: TLS started on ESMTP session between client <*client-side interface-name*>:<*client IP address*>/<*client port*> and server <*server-side interface-name*>:<*server IP address*>/<*server port*> *Also available in Version 7.2(3).*
High Availability Features	
Added Dataplane Keepalive Mechanism	You can now configure the security appliance so that a failover will not occur if the AIP SSM is upgraded. In previous releases when two security appliances with AIP SSMs are configured in failover and the AIP SSM software is updated, the security appliance triggers a failover, because the AIP SSM needs to reboot or restart for the software update to take effect. *Also available in Version 7.0(7) and 7.2(3)*
Fully Qualified Domain Name Support Enhancement	Added option in the **redirect-fqdn** command to send either the fully qualified domain name (FQDN) or the IP address to the client in a VPN load balancing cluster.
DHCP Features	
DHCP client ID enhancement	If you enable the DHCP client for an interface using the **ip address dhcp** command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use this new command to include the interface MAC address for option 61. If you do not configure this command, the client ID is as follows: cisco-<MAC>-<interface>-<hostname>. We introduced the following command: **dhcp-client client-id interface** *interface_name* *Also available in Version 7.2(3).*

Table 1-4 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
DHCP client broadcast flag	If you enable the DHCP client for an interface using the **ip address dhcp** command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1. If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address. The DHCP client can receive both broadcast and unicast offers from the DHCP server. We introduced the following command: **dhcp-client broadcast-flag**
Platform Features	
ASA 5510 Security Plus License Allows Gigabit Ethernet for Port 0 and 1	The ASA 5510 security appliance now has the security plus license to enable GE (Gigabit Ethernet) for port 0 and 1. If you upgrade the license from base to security plus, the capacity of the external port Ethernet0/0 and Ethernet0/1 increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** command to change the speed on the interface and use the **show interface** command to see what speed is currently configured for each interface. *Also available in Version 7.2(3).*
ASA 5505 Increased VLAN range	The ASA 5505 security appliance now supports VLAN IDs between 1 and 4090. Originally, only VLAN IDs between 1 and 1001 were supported. *Also available in Version 7.2(3).*
Troubleshooting Features	
capture Command Enhancement	The enhancement to the **capture** command allows the user to capture traffic and display it in real time. It also allows the user to specify command line options to filter traffic without having to configure a separate access list. This enhancement adds the **real-time** and five-tupple **match** options. **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] *Also available in Version 7.2(3).*

Table 1-4 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
ASDM Features	
ASDM banner enhancement	The adaptive security appliance software supports an ASDM banner. If configured, when you start ASDM, this banner text will appear in a dialog box with the option to continue or disconnect. The Continue option dismisses the banner and completes login as usual whereas, the Disconnect option dismisses the banner and terminates the connection. This enhancement requires the customer to accept the terms of a written policy before connecting. Following is the new CLI associated with this enhancement: **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** *Also available in Version 7.2(3).*

New Features in Version 8.0(2)

Released: June 18, 2007

Table 1-5 lists the new features forASA and PIX Version 8.0(2).

Note There was no 8.0(1) release.

Table 1-5 New Features for ASA and PIX Version 8.0(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.

Table 1-5 New Features for ASA and PIX Version 8.0(2) (continued)

Feature	Description
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 adaptive 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.
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	

Table 1-5 New Features for ASA and PIX Version 8.0(2) (continued)

Feature	Description
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	
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	

Table 1-5 New Features for ASA and PIX Version 8.0(2) (continued)

Feature	Description
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 adaptive 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.
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.

Table 1-5 New Features for ASA and PIX Version 8.0(2) (continued)

Feature	Description
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.
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.

Table 1-5 New Features for ASA and PIX Version 8.0(2) (continued)

Feature	Description
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 adaptive 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 adaptive security appliance.

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

Firewall Functional Overview

Firewalls protect inside networks from unauthorized access by users on an outside network. A firewall can also protect inside networks from each other, for example, by keeping a human resources network separate from a user network. If you have network resources that need to be available to an outside user, such as a web or FTP server, you can place these resources on a separate network behind the firewall, called a *demilitarized zone* (DMZ). The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the other inside networks. You can also control when inside users access outside networks (for example, access to the Internet), by allowing only certain addresses out, by requiring authentication or authorization, or by coordinating with an external URL filtering server.

When discussing networks connected to a firewall, the *outside* network is in front of the firewall, the *inside* network is protected and behind the firewall, and a *DMZ*, while behind the firewall, allows limited access to outside users. Because the security appliance lets you configure many interfaces with varied security policies, including many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

This section includes the following topics:

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the security appliance allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level). You can apply actions to traffic to customize the security policy. This section includes the following topics:

Permitting or Denying Traffic with Access Lists

You can apply an access list to limit traffic from inside to outside, or allow traffic from outside to inside. For transparent firewall mode, you can also apply an EtherType access list to allow non-IP traffic.

Applying NAT

Some of the benefits of NAT include the following:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.

Protecting from IP Fragments

The security appliance provides IP fragment protection. This feature performs full reassembly of all ICMP error messages and virtual reassembly of the remaining IP fragments that are routed through the security appliance. Fragments that fail the security check are dropped and logged. Virtual reassembly cannot be disabled.

Using AAA for Through Traffic

You can require authentication and/or authorization for certain types of traffic, for example, for HTTP. The security appliance also sends accounting information to a RADIUS or TACACS+ server.

Applying HTTP, HTTPS, or FTP Filtering

Although you can use access lists to prevent outbound access to specific websites or FTP servers, configuring and managing web usage this way is not practical because of the size and dynamic nature of the Internet. We recommend that you use the security appliance in conjunction with a separate server running one of the following Internet filtering products:

- Websense Enterprise
- Secure Computing SmartFilter

Applying Application Inspection

Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the security appliance to do a deep packet inspection.

Sending Traffic to the Advanced Inspection and Prevention Security Services Module

If your model supports the AIP SSM for intrusion prevention, then you can send traffic to the AIP SSM for inspection. The AIP SSM is an intrusion prevention services module that monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. Other legitimate connections continue to operate independently without interruption. For more information, see *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*.

Sending Traffic to the Content Security and Control Security Services Module

If your model supports it, the CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that you configure the adaptive security appliance to send to it.

Applying QoS Policies

Some network traffic, such as voice and streaming video, cannot tolerate long latency times. QoS is a network feature that lets you give priority to these types of traffic. QoS refers to the capability of a network to provide better service to selected network traffic.

Applying Connection Limits and TCP Normalization

You can limit TCP and UDP connections and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. The security appliance uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

TCP normalization is a feature consisting of advanced TCP connection settings designed to drop packets that do not appear normal.

Enabling Threat Detection

You can configure scanning threat detection and basic threat detection, and also how to use statistics to analyze threats.

Basic threat detection detects activity that might be related to an attack, such as a DoS attack, and automatically sends a system log message.

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the security appliance scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

You can configure the security appliance to send system log messages about an attacker or you can automatically shun the host.

Firewall Mode Overview

The security appliance runs in two different firewall modes:

- Routed
- Transparent

In routed mode, the security appliance is considered to be a router hop in the network.

In transparent mode, the security appliance acts like a "bump in the wire," or a "stealth firewall," and is not considered a router hop. The security appliance connects to the same network on its inside and outside interfaces.

You might use a transparent firewall to simplify your network configuration. Transparent mode is also useful if you want the firewall to be invisible to attackers. You can also use a transparent firewall for traffic that would otherwise be blocked in routed mode. For example, a transparent firewall can allow multicast streams using an EtherType access list.

Stateful Inspection Overview

All traffic that goes through the security appliance is inspected using the Adaptive Security Algorithm and either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process.

A stateful firewall like the security appliance, however, takes into consideration the state of a packet:

- Is this a new connection?

  If it is a new connection, the security appliance has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path."

  The session management path is responsible for the following tasks:

  - Performing the access list checks

  - Performing route lookups
  - Allocating NAT translations (xlates)
  - Establishing sessions in the “fast path”

Note The session management path and the fast path make up the “accelerated security path.”

Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that have two or more channels: a data channel, which uses well-known port numbers, and a control channel, which uses different port numbers for each session. These protocols include FTP, H.323, and SNMP.

- Is this an established connection?

  If the connection is already established, the security appliance does not need to re-check packets; most matching packets can go through the fast path in both directions. The fast path is responsible for the following tasks:

  - IP checksum verification
  - Session lookup
  - TCP sequence number check
  - NAT translations based on existing sessions
  - Layer 3 and Layer 4 header adjustments

  For UDP or other connectionless protocols, the security appliance creates connection state information so that it can also use the fast path.

  Data packets for protocols that require Layer 7 inspection can also go through the fast path.

  Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection.

VPN Functional Overview

A VPN is a secure connection across a TCP/IP network (such as the Internet) that appears as a private connection. This secure connection is called a tunnel. The security appliance uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The security appliance functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination. The security appliance invokes various standard protocols to accomplish these functions.

The security appliance performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data

- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

The security appliance invokes various standard protocols to accomplish these functions.

Security Context Overview

You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

In multiple context mode, the security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs into the admin context, then that user has system administrator rights and can access the system and all other contexts.

Note You can run all your contexts in routed mode or transparent mode; you cannot run some contexts in one mode and others in another.

Multiple context mode supports static routing only. For more information about multiple context mode, see Chapter 4, “Enabling Multiple Context Mode.”