CHAPTER 1

Introduction to the Cisco ASA 5500 Series Adaptive Security Appliance

The adaptive 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/SSC or an integrated content security and control module called the CSC SSM. The adaptive 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 VPN, SSL VPN, and clientless SSL VPN support, and many more features.

This chapter includes the following sections:

ASA 5500 Model Support

For a complete list of supported ASA models for this release, see *Cisco ASA 5500 Series Hardware and Software Compatibility*:

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

Module Support

For a complete list of supported modulesfor this release, see *Cisco ASA 5500 Series Hardware and Software Compatibility*:

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

VPN Specifications

See the *Supported VPN Platforms, Cisco ASA 5500 Series*:

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

New Features

- This section includes the following topics:New Features in Version 8.3(2), page 1-5
- New Features in Version 8.3(1), page 1-7

Note New, changed, and deprecated syslog messages are listed in *Cisco ASA 5500 Series System Log Messages*.

Released: March 4, 2011

Table 1-1 lists the new features for ASA Version 8.2(4.4).

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Table 1-1 New Features for ASA Version 8.2(4.4)

Feature	Description
Hardware Features	
Support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X	We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10.
Remote Access Features	
Clientless SSL VPN support for Outlook Web Access 2010	By default, Clientless SSL VPN now provides content transformation (rewriting) support for Outlook Web Access (OWA) 2010 traffic. We did not modify any commands.

Released: January 18, 2011

Table 1-2 lists the new features for ASA Version 8.2(4.1).

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Table 1-2 New Features for ASA Version 8.2(4.1)

Feature	Description
Remote Access Features	
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommended). This release does not support SHA-2 for other uses or products. This feature does not involve configuration changes. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. To support this feature, we added the Signature Algorithm field to the **show crypto ca certificate** command to identify the digest algorithm used when generating the signature.

Released: December 15, 2010

Table 1-3 lists the new features for ASA Version 8.2(4).

Table 1-3 New Features for ASA Version 8.2(4)

Feature	Description
Hardware Features	
Support for the Cisco ASA 5585-X with SSP-10 and SSP-40	We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10 and -40. **Note** The ASA 5585-X is not supported in Version 8.3(x).

Released: November 2, 2010

Table 1-4 lists the new features for ASA interim Version 8.2(3.9).

Note We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

Table 1-4 New Features for ASA Version 8.2(3.9)

Feature	Description
Remote Access Features	
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommended). This release does not support SHA-2 for other uses or products. This feature does not involve configuration changes. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. To support this feature, we added the Signature Algorithm field to the **show crypto ca certificate** command to identify the digest algorithm used when generating the signature.

Released: August 9, 2010

Table 1-5Table 1-5 lists the new features for ASA Version 8.2(3).

Table 1-5 New Features for ASA Version 8.2(3)

Feature	Description
Hardware Features	
Support for the Cisco ASA 5585-X with SSP-20 and SSP-60	Support for the ASA 5585-X with Security Services Processor (SSP)-20 and -60 was introduced. **Note** The ASA 5585-X is not supported in Version 8.3(x).
Remote Access Features	
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware. **Note** For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment. **Note** The ASA 5580/5585-X platforms already integrate this capability; therefore, crypto engine commands are not applicable on these platforms. The following commands were introduced or modified: **crypto engine large-mod-accel**, **clear configure crypto engine**, **show running-config crypto engine**, and **show running-config crypto**. *Also available in Version 8.3(2).*

Table 1-5 New Features for ASA Version 8.2(3) (continued)

Feature	Description
Microsoft Internet Explorer proxy lockdown control	Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged; the default setting for the tab can be shown or hidden, depending on the user registry settings. The following command was introduced: **msie-proxy lockdown**.
Trusted Network Detection Pause and Resume	This feature enables the AnyConnect client to retain its session information and cookie so that it can seamlessly restore connectivity after the user leaves the office, as long as the session does not exceed the idle timer setting. This feature requires an AnyConnect release that supports TND pause and resume.

New Features in Version 8.3(2)

Released: August 2, 2010

Table 1-6 lists the new features forASA Version 8.3(2).

Table 1-6 New Features for ASA Version 8.3(2)

Feature	Description
Monitoring Features	
Enhanced logging and connection blocking	When you configure a syslog server to use TCP, and the syslog server is unavailable, the adaptive security appliance blocks new connections that generate syslog messages until the server becomes available again (for example, VPN, firewall, and cut-through-proxy connections). This feature has been enhanced to also block new connections when the logging queue on the adaptive security appliance is full; connections resume when the logging queue is cleared. This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommend allowing new connections when syslog messages cannot be sent. To allow new connections, configure the syslog server to use UDP or use the **logging permit-hostdown** command. The following commands were modified: **show logging**. The following syslog messages were introduced: 414005, 414006, 414007, and 414008
Remote Access Features	

Table 1-6 New Features for ASA Version 8.3(2) (continued)

Feature	Description
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware. **Note** For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment. The following commands were introduced or modified: **crypto engine large-mod-accel**, **clear configure crypto engine**, **show running-config crypto engine**, and **show running-config crypto**. *Also available in Version 8.2(3).*
Microsoft Internet Explorer proxy lockdown control	Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged; the default setting for the tab can be shown or hidden, depending on the user registry settings. The following command was introduced: **msie-proxy lockdown**. *Also available in Version 8.2(3).*
Secondary password enhancement	You can now configure SSL VPN support for a common secondary password for all authentications or use the primary password as the secondary password. The following command was modified: **secondary-pre-fill-username** [**use-primary-password** | **use-common-password**]]

Table 1-6 New Features for ASA Version 8.3(2) (continued)

Feature	Description
General Features	

No Payload Encryption image for export	For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. For version 8.3(2), you can now install a No Payload Encryption image (asa832-npe-k8.bin) on the following models:
	• ASA 5505
	• ASA 5510
	• ASA 5520
	• ASA 5540
	• ASA 5550
	Features that are disabled in the No Payload Encryption image include:
	• Unified Communications.
	• Strong encryption for VPN (DES encryption is still available for VPN).
	• VPN load balancing (note that the CLI is still present; the feature will not function, however).
	• Downloading of the dynamic database for the Botnet Traffic Filer (Static black and whitelists are still supported. Note that the CLI is still present; the feature will not function, however.).
	• Management protocols requiring strong encryption, including SSL, SSHv2, and SNMPv3. You can, however, use SSL or SNMPv3 using base encryption (DES). Also, SSHv1 and SNMPv1 and v2 are still available.
	If you attempt to install a Strong Encryption (3DES/AES) license, you see the following warning:
	`WARNING: Strong encryption types have been disabled in this image; the`
	`VPN-3DES-AES license option has been ignored.`

New Features in Version 8.3(1)

Released: March 8, 2010

Table 1-7 lists the new features forASA Version 8.3(1).

Table 1-7 New Features for ASA Version 8.3(1)

Feature	Description
Remote Access Features	
Smart Tunnel Enhancements	Logoff enhancement—Smart tunnel can now be logged off when all browser windows have been closed (parent affinity), or you can right click the notification icon in the system tray and confirm log out. Tunnel Policy—An administrator can dictate which connections go through the VPN gateway and which do not. An end user can browse the Internet directly while accessing company internal resources with smart tunnel if the administrator chooses. Simplified configuration of which applications to tunnel—When a smart tunnel is required, a user no longer needs to configure a list of processes that can access smart tunnel and in turn access certain web pages. An “enable smart tunnel” check box for either a bookmark or standalone application allows for an easier configuration process. Group policy home page—Using a check box in ASDM, administrators can now specify their home page in group policy in order to connect via smart tunnel. The following commands were introduced: **smart-tunnel network**, **smart-tunnel tunnel-policy**.
Newly Supported Platforms for Browser-based VPN	Release 8.3(1) provides browser-based (clientless) VPN access from the following newly supported platforms: • Windows 7 x86 (32-bit) and x64 (64-bit) via Internet Explorer 8.x and Firefox 3.x • Windows Vista x64 via Internet Explorer 7.x/8.x, or Firefox 3.x. • Windows XP x64 via Internet Explorer 6.x/7.x/8.x and Firefox 3.x • Mac OS 10.6.x 32- and 64-bit via Safari 4.x and Firefox 3.x. Firefox 2.x is likely to work, although we no longer test it. Release 8.3(1) introduces browser-based support for 64-bit applications on Mac OS 10.5. Release 8.3(1) now supports smart tunnel access on all 32-bit and 64-bit Windows OSs supported for browser-based VPN access, Mac OS 10.5 running on an Intel processor only, and Mac OS 10.6.x. The adaptive security appliance does not support port forwarding on 64-bit OSs. Browser-based VPN access does not support Web Folders on Windows 7, Vista, and Internet Explorer 8. An ActiveX version of the RDP plug-in is not available for 64-bit browsers. **Note** Windows 2000 and Mac OS X 10.4 are no longer supported for browser-based access.

Table 1-7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
IPv6 support for IKEv1 LAN-to-LAN VPN connections	For LAN-to-LAN connections using mixed IPv4 and IPv6 addressing, or all IPv6 addressing, the adaptive security appliance supports VPN tunnels if both peers are Cisco ASA 5500 series adaptive security appliances, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6). Specifically, the following topologies are supported when both peers are Cisco ASA 5500 series adaptive security appliances: • The adaptive security appliances have IPv4 inside networks and the outside network is IPv6 (IPv4 addresses on the inside interfaces and IPv6 addresses on the outside interfaces). • The adaptive security appliances have IPv6 inside networks and the outside network is IPv4 (IPv6 addresses on the inside interface and IPv4 addresses on the outside interfaces). • The adaptive security appliances have IPv6 inside networks and the outside network is IPv6 (IPv6 addresses on the inside and outside interfaces). **Note** The defect CSCtd38078 currently prevents the Cisco ASA 5500 series from connecting to a Cisco IOS device as the peer device of a LAN-to-LAN connection. The following commands were modified or introduced: **isakmp enable**, **crypto map**, **crypto dynamic-map**, **tunnel-group**, **ipv6-vpn-filter**, **vpn-sessiondb**, **show crypto isakmp sa**, **show crypto ipsec sa**, **show crypto debug-condition**, **show debug crypto**, **show vpn-sessiondb**, **debug crypto condition**, **debug menu ike**.
Firewall Features	
Interface-Independent Access Policies	You can now configure access rules that are applied globally, as well as access rules that are applied to an interface. If the configuration specifies both a global access policy and interface-specific access policies, the interface-specific policies are evaluated before the global policy. The following command was modified: **access-group global**.
Network and Service Objects	You can now create named network objects that you can use in place of a host, a subnet, or a range of IP addresses in your configuration and named service objects that you can use in place of a protocol and port in your configuration. You can then change the object definition in one place, without having to change any other part of your configuration. This release introduces support for network and service objects in the following features: • NAT • Access lists • Network object groups The following commands were introduced or modified: **object network**, **object service**, **show running-config object**, **clear configure object**, **access-list extended**, **object-group network**.

Table 1-7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
Object-group Expansion Rule Reduction	Significantly reduces the network object-group expansion while maintaining a satisfactory level of packet classification performance. The following commands were modified: **show object-group**, **clear object-group**, **show access-list**.
NAT Simplification	The NAT configuration was completely redesigned to allow greater flexibility and ease of use. You can now configure NAT using auto NAT, where you configure NAT as part of the attributes of a network object, and manual NAT, where you can configure more advanced NAT options. The following commands were introduced or modified: **nat** (in global and object network configuration mode), **show nat**, **show nat pool**, **show xlate**, **show running-config nat**. The following commands were removed: **global**, **static**, **nat-control**, **alias**.
Use of Real IP addresses in access lists instead of translated addresses	When using NAT, mapped addresses are no longer required in an access list for many features. You should always use the real, untranslated addresses when configuring these features. Using the real address means that if the NAT configuration changes, you do not need to change the access lists. The following commands and features that use access lists now use real IP addresses. These features are automatically migrated to use real IP addresses when you upgrade to 8.3, unless otherwise noted. • **access-group** command • Modular Policy Framework **match access-list** command • Botnet Traffic Filter **dynamic-filter enable classify-list** command • AAA **aaa ... match** commands • WCCP **wccp redirect-list group-list** command **Note** WCCP is not automatically migrated when you upgrade to 8.3.
Threat Detection Enhancements	You can now customize the number of rate intervals for which advanced statistics are collected. The default number of rates was changed from 3 to 1. For basic statistics, advanced statistics, and scanning threat detection, the memory usage was improved. The following commands were modified: **threat-detection statistics port number-of-rates**, **threat-detection statistics protocol number-of-rates**, **show threat-detection memory**.
Unified Communication Features	
SCCP v19 support	The IP phone support in the Cisco Phone Proxy feature was enhanced to include support for version 19 of the SCCP protocol on the list of supported IP phones.

Table 1-7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
Cisco Intercompany Media Engine Proxy	Cisco Intercompany Media Engine (UC-IME) enables companies to interconnect on-demand, over the Internet with advanced features made available by VoIP technologies. Cisco Intercompany Media Engine allows for business-to-business federation between Cisco Unified Communications Manager clusters in different enterprises by utilizing peer-to-peer, security, and SIP protocols to create dynamic SIP trunks between businesses. A collection of enterprises work together to end up looking like one large business with inter-cluster trunks between them. The following commands were modified or introduced: **uc-ime**, **fallback hold-down**, **fallback monitoring**, **fallback sensitivity-file**, **mapping-service listening-interface**, **media-termination**, **ticket epoch**, **ucm address**, **clear configure uc-ime**, **debug uc-ime**, **show running-config uc-ime**, **inspect sip**.
SIP Inspection Support for IME	SIP inspection has been enhance to support the new Cisco Intercompany Media Engine (UC-IME) Proxy. The following command was modified: **inspect sip**.
Monitoring Features	
Time Stamps for Access List Hit Counts	Displays the timestamp, along with the hash value and hit count, for a specified access list. The following command was modified: **show access-list**.
High Performance Monitoring for ASDM	You can now enable high performance monitoring for ASDM to show the top 200 hosts connected through the adaptive security appliance. Each entry of a host contains the IP address of the host and the number of connections initiated by the host, and is updated every 120 seconds. The following commands were introduced: **hpm topn enable**, **clear configure hpm**, **show running-config hpm**.
Licensing Features	
Non-identical failover licenses	Failover licenses no longer need to be identical on each unit. The license used for both units is the combined license from the primary and secondary units. **Note** For the ASA 5505 and 5510 adaptive security appliances, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license. The following commands were modified: **show activation-key** and **show version**.

Table 1-7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
Stackable time-based licenses	Time-based licenses are now stackable. In many cases, you might need to renew your time-based license and have a seamless transition from the old license to the new one. For features that are only available with a time-based license, it is especially important that the license not expire before you can apply the new license. The adaptive security appliance allows you to *stack* time-based licenses so you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early. For licenses with numerical tiers, stacking is only supported for licenses with the same capacity, for example, two 1000-session SSL VPN licenses. You can view the state of the licenses using the show activation-key command.
Intercompany Media Engine License	The IME license was introduced.
Multiple time-based licenses active at the same time	You can now install multiple time-based licenses, and have one license per feature active at a time. The following commands were modified: **show activation-key** and **show version**.
Discrete activation and deactivation of time-based licenses.	You can now activate or deactivate time-based licenses using a command. The following command was modified: **activation-key** [**activate** | **deactivate**].
General Features	
Master Passphrase	The master passphrase feature allows you to securely store plain text passwords in encrypted format. It provides a master key that is used to universally encrypt or mask all passwords, without changing any functionality. The following commands were introduced: **key config-key password-encryption**, **password encryption aes**.

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 adaptive 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, page 1-13
- Firewall Mode Overview, page 1-16
- Stateful Inspection Overview, page 1-16

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the adaptive 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, page 1-13
- Applying NAT, page 1-13
- Protecting from IP Fragments, page 1-14
- Using AAA for Through Traffic, page 1-14
- Applying HTTP, HTTPS, or FTP Filtering, page 1-14
- Applying Application Inspection, page 1-14
- Sending Traffic to the Advanced Inspection and Prevention Security Services Module, page 1-14
- Sending Traffic to the Content Security and Control Security Services Module, page 1-14
- Applying QoS Policies, page 1-15
- Applying Connection Limits and TCP Normalization, page 1-15
- Enabling Threat Detection, page 1-15
- Enabling the Botnet Traffic Filter, page 1-15
- Configuring Cisco Unified Communications, page 1-15

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

Enabling the Botnet Traffic Filter

Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses (the blacklist), and then logs any suspicious activity. When you see syslog messages about the malware activity, you can take steps to isolate and disinfect the host.

Configuring Cisco Unified Communications

The Cisco ASA 5500 Series appliances are a strategic platform to provide proxy functions for unified communications deployments. The purpose of a proxy is to terminate and reoriginate connections between a client and server. The proxy delivers a range of security functions such as traffic inspection, protocol conformance, and policy control to ensure security for the internal network. An increasingly popular function of a proxy is to terminate encrypted connections in order to apply security policies while maintaining confidentiality of connections.

Firewall Mode Overview

The adaptive security appliance runs in two different firewall modes:

- Routed
- Transparent

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

In transparent mode, the adaptive security appliance acts like a "bump in the wire," or a "stealth firewall," and is not considered a router hop. The adaptive 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 adaptive 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.

Note The TCP state bypass feature allows you to customize the packet flow. See the "TCP State Bypass" section on page 49-3.

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

- Is this a new connection?

  If it is a new connection, the adaptive 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"

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

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

Security Context Overview

You can partition a single adaptive 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 adaptive 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 adaptive 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.