CHAPTER 1

Introduction to the Cisco ASA 5500 Series

The ASA provides advanced Stateful Firewall and VPN concentrator functionality in one device, and for some models, an integrated Intrusion Prevention System (IPS) module or an integrated Content Security and Control (CSC) module. The ASA 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, clientless SSL VPN support, and many more features.

This chapter includes the following sections:

Hardware and Software Compatibility

For a complete list of supported hardware and software, see the *Cisco ASA Compatibility*:

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

VPN Specifications

See *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:

Note New, changed, and deprecated syslog messages are listed in syslog message guide.

Note Version 8.4(4) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.1) or later.

New Features in Version 8.6(1)

Released: February 28, 2012

Table 1-1 lists the new features for ASA Version 8.6(1). This ASA software version is only supported on the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.

Note Version 8.6(1) includes all features in 8.4(2), plus the features listed in this table.

Features added in 8.4(3) are not included in 8.6(1) unless they are explicitly listed in this table.

Table 1-1 New Features forASA Version 8.6(1)

Feature	Description
Hardware Features	
Support for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.
IPS Features	
Support for the IPS SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the IPS SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. We introduced or modified the following commands: **session**, **show module**, **sw-module**.
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. *Also available in Version 8.4(3).*

Table 1-1 New Features forASA Version 8.6(1) (continued)

Feature	Description
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** | **none**] and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. *Also available in Version 8.4(3).*
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout. We introduced the following commands: **vpn-session-timeout alert-interval**, **vpn-idle-timeout alert-interval**. *Also available in Version 8.4(3).*
Multiple Context Mode Features	
Automatic generation of a MAC address prefix	In multiple context mode, the ASA now converts the automatic MAC address generation configuration to use a default prefix. The ASA auto-generates the prefix based on the last two bytes of the interface MAC address. This conversion happens automatically when you reload, or if you reenable MAC address generation. The prefix method of generation provides many benefits, including a better guarantee of unique MAC addresses on a segment. You can view the auto-generated prefix by entering the **show running-config mac-address** command. If you want to change the prefix, you can reconfigure the feature with a custom prefix. The legacy method of MAC address generation is no longer available. **Note** To maintain hitless upgrade for failover pairs, the ASA does *not* convert the MAC address method in an existing configuration upon a reload if failover is enabled. However, we strongly recommend that you manually change to the prefix method of generation. After upgrading, to use the prefix method of MAC address generation, reenable MAC address generation to use the default prefix. We modified the following command: **mac-address auto**.
AAA Features	
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this command in aaa-server host configuration mode). *Also available in Version 8.4(3).*

Table 1-1 New Features forASA Version 8.6(1) (continued)

Feature	Description
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values. *Also available in Version 8.4(3).*
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*. *Also available in Version 8.4(3).*

New Features in Version 8.4(5)

New Features in Version 8.4(4.1)

Released: June 18, 2012

Table 1-2 lists the new features for ASA Version 8.4(4.1).

Note Version 8.4(4) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.1) or later.

Table 1-2 New Features for ASA Version 8.4(4.1)

Feature	Description
Certification Features	
FIPS and Common Criteria certifications	The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 FIPS 140-2 validation for the Cisco ASA 5500 series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, and ASA 5585-X. The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which provides the basis for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform solutions. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Table 1-2 New Features for ASA Version 8.4(4.1) (continued)

Feature	Description
Support for administrator password policy when using the local database	When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters. We introduced or modified the following commands: **change-password**, **password-policy lifetime**, **password-policy minimum changes**, **password-policy minimum-length**, **password-policy minimum-lowercase**, **password-policy minimum-uppercase**, **password-policy minimum-numeric**, **password-policy minimum-special**, **password-policy authenticate enable**, **clear configure password-policy**, **show running-config password-policy**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Support for SSH public key authentication	You can now enable public key authentication for SSH connections to the ASA on a per-user basis using Base64 key up to 2048 bits. We introduced the following commands: **ssh authentication**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported. We introduced the following command: **ssh key-exchange**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Support for a maximum number of management sessions	You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions. We introduced the following commands: **quota management-session**, **show running-config quota management-session**, **show quota management-session**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Table 1-2 New Features for ASA Version 8.4(4.1) (continued)

Feature	Description

Additional ephemeral Diffie-Hellman ciphers for SSL encryption	The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher suites:
	• DHE-AES128-SHA1
	• DHE-AES256-SHA1
	These cipher suites are specified in RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.
	When supported by the client, DHE is the preferred cipher because it provides Perfect Forward Secrecy. See the following limitations:
	• DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS 1.0 for the SSL server.
	`!! set server version`
	`hostname(config)#` **`ssl server-version tlsv1 sslv3`**
	`!! set client version`
	`hostname(config) #` **`ssl client-version any`**
	• Some popular applications do not support DHE, so include at least one other SSL encryption method to ensure that a cipher suite common to both the SSL client and server can be used.
	• Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Secure Desktop, and Internet Explorer 9.0.
	We modified the following command: **ssl encryption**.
	This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).

Image verification	Support for SHA-512 image integrity checking was added. We modified the following command: **verify**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Improved pseudo-random number generation	Hardware-based noise for additional entropy was added to the software-based random number generation process. This change makes pseudo-random number generation (PRNG) more random and more difficult for attackers to get a repeatable pattern or guess the next random number to be used for encryption and decryption operations. Two changes were made to improve PRNG: • Use the current hardware-based RNG for random data to use as one of the parameters for software-based RNG. • If the hardware-based RNG is not available, use additional hardware noise sources for software-based RNG. Depending on your model, the following hardware sensors are used: – ASA 5505—Voltage sensors. – ASA 5510 and 5550—Fan speed sensors. – ASA 5520, 5540, and 5580—Temperature sensors. – ASA 5585-X—Fan speed sensors. We introduced the following commands: **show debug menu cts** [**128** | **129**] *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
Remote Access Features	

Table 1-2 New Features for ASA Version 8.4(4.1) (continued)

Feature	Description
Clientless SSL VPN: Enhanced quality for rewriter engines	The clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN users. We did not add or modify any commands for this feature. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Failover Features	
Configure the connection replication rate during a bulk sync	You can now configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASA is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synced. We introduced the following command: **failover replication rate** *rate*. *This feature is not available in 8.6(1) or 8.7(1). This feature is also in 8.5(1.7).*
Application Inspection Features	
SunRPC change from dynamic ACL to pin-hole mechanism	Previously, Sun RPC inspection does not support outbound access lists because the inspection engine uses dynamic access lists instead of secondary connections. In this release, when you configure dynamic access lists on the ASA, they are supported on the ingress direction only and the ASA drops egress traffic destined to dynamic ports. Therefore, Sun RPC inspection implements a pinhole mechanism to support egress traffic. Sun RPC inspection uses this pinhole mechanism to support outbound dynamic access lists. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Inspection reset action change	Previously, when the ASA dropped a packet due to an inspection engine rule, the ASA sent only one RST to the source device of the dropped packet. This behavior could cause resource issues. In this release, when you configure an inspection engine to use a reset action and a packet triggers a reset, the ASA sends a TCP reset under the following conditions: • The ASA sends a TCP reset to the inside host when the **service resetoutbound** command is enabled. (The **service resetoutbound** command is disabled by default.) • The ASA sends a TCP reset to the outside host when the **service resetinbound** command is enabled. (The **service resetinbound** command is disabled by default.) For more information, see the **service** command in the ASA *Cisco ASA 5500 Series Command Reference*. This behavior ensures that a reset action will reset the connections on the ASA and on inside servers; therefore countering denial of service attacks. For outside hosts, the ASA does not send a reset by default and information is not revealed through a TCP reset. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Module Features	

Table 1-2 New Features for ASA Version 8.4(4.1) (continued)

Feature	Description
ASA 5585-X support for the ASA CX SSP-10 and -20	The ASA CX module lets you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees. We introduced or modified the following commands: **capture**, **cxsc**, **cxsc auth-proxy**, **debug cxsc**, **hw-module module password-reset**, **hw-module module reload**, **hw-module module reset**, **hw-module module shutdown**, **session do setup host ip, session do get-config, session do password-reset, show asp table classify domain cxsc**, **show asp table classify domain cxsc-auth-proxy**, **show capture**, **show conn**, **show module**, **show service-policy**.
ASA 5585-X support for network modules	The ASA 5585-X now supports additional interfaces on network modules in slot 1. You can install one or two of the following optional network modules: • ASA 4-port 10G Network Module • ASA 8-port 10G Network Module • ASA 20-port 1G Network Module *This feature is not available in 9.0(1), 9.0(2), or 9.1(1).*

New Features in Version 8.4(3)

Released: January 9, 2012

Table 1-3 lists the new features for ASA Version 8.4(3).

Table 1-3 New Features for ASA Version 8.4(3)

Feature	Description
NAT Features	
Round robin PAT pool allocation uses the same IP address for existing hosts	When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. We did not modify any commands. *This feature is not available in 8.5(1) or 8.6(1).*

Table 1-3 New Features for ASA Version 8.4(3) (continued)

Feature	Description
Flat range of PAT ports for a PAT pool	If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool. If you have a lot of traffic that uses the lower port ranges, when using a PAT pool, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535. We modified the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] (object network configuration mode) and **nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] (global configuration mode). *This feature is not available in 8.5(1) or 8.6(1).*
Extended PAT for a PAT pool	Each PAT IP address allows up to 65535 ports. If 65535 ports do not provide enough translations, you can now enable extended PAT for a PAT pool. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. We modified the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**extended**]] (object network configuration mode) and **nat source dynamic** [**pat-pool** *mapped_object* [**extended**]] (global configuration mode). *This feature is not available in 8.5(1) or 8.6(1).*
Configurable timeout for PAT xlate	When a PAT xlate times out (by default after 30 seconds), and the ASA reuses the port for a new translation, some upstream routers might reject the new connection because the previous connection might still be open on the upstream device. The PAT xlate timeout is now configurable, to a value between 30 seconds and 5 minutes. We introduced the following command: **timeout pat-xlate**. *This feature is not available in 8.5(1) or 8.6(1).*

Table 1-3 New Features for ASA Version 8.4(3) (continued)

Feature	Description
Automatic NAT rules to translate a VPN peer's local IP address back to the peer's real IP address	In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address. You can enable this feature on one interface per tunnel group. Object NAT rules are dynamically added and deleted when the VPN session is established or disconnected. You can view the rules using the **show nat** command. **Note** Because of routing issues, we do not recommend using this feature unless you know you need this feature; contact Cisco TAC to confirm feature compatibility with your network. See the following limitations: • Only supports Cisco IPsec and AnyConnect Client. • Return traffic to the public IP addresses must be routed back to the ASA so the NAT policy and VPN policy can be applied. • Does not support load-balancing (because of routing issues). • Does not support roaming (public IP changing). We introduced the following command: **nat-assigned-to-public-ip** *interface* (tunnel-group general-attributes configuration mode).
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4.
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** | **none**] and **anyconnect ssl compression** [**deflate** | **lzs** | **none**].
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout. We introduced the following commands: **vpn-session-timeout alert-interval**, **vpn-idle-timeout alert-interval**.
AAA Features	

Table 1-3 New Features for ASA Version 8.4(3) (continued)

Feature	Description
Increased maximum LDAP values per attribute	The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037. We introduced the following command: **ldap-max-value-range** *number* (Enter this command in aaa-server host configuration mode).
Support for sub-range of LDAP search results	When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.
Key vendor-specific attributes (VSAs) sent in RADIUS access request and accounting request packets from the ASA	Four New VSAs—Tunnel Group Name (146) and Client Type (150) are sent in RADIUS access request packets from the ASA. Session Type (151) and Session Subtype (152) are sent in RADIUS accounting request packets from the ASA. All four attributes are sent for all accounting request packet types: Start, Interim-Update, and Stop. The RADIUS server (for example, ACS and ISE) can then enforce authorization and policy attributes or use them for accounting and billing purposes.
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*.

New Features in Version 8.4(2)

Released: June 20, 2011

Table 1-4 lists the new features for ASA Version 8.4(2).

Table 1-4 New Features for ASA Version 8.4(2)

Feature	Description
Firewall Features	
Identity Firewall	Typically, a firewall is not aware of the user identities and, therefore, cannot apply security policies based on identity. The Identity Firewall in the ASA provides more granular access control based on users' identities. You can configure access rules and security policies based on usernames and user groups name rather than through source IP addresses. The ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped usernames instead of network IP addresses. The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping. The ASA uses Windows Active Directory as the source to retrieve the current user identity information for specific IP addresses. In an enterprise, some users log onto the network by using other authentication mechanisms, such as authenticating with a web portal (cut-through proxy) or by using a VPN. You can configure the Identity Firewall to allow these types of authentication in connection with identity-based access policies. We introduced or modified the following commands: **user-identity enable**, **user-identity default-domain**, **user-identity domain**, **user-identity logout-probe**, **user-identity inactive-user-timer**, **user-identity poll-import-user-group-timer**, **user-identity action netbios-response-fail**, **user-identity user-not-found**, **user-identity action ad-agent-down**, **user-identity action mac-address-mismatch**, **user-identity action domain-controller-down**, **user-identity ad-agent active-user-database**, **user-identity ad-agent hello-timer**, **user-identity ad-agent aaa-server**, **user-identity update import-user**, **user-identity static user**, **ad-agent-mode**, **dns domain-lookup**, **dns poll-timer**, **dns expire-entry-timer**, **object-group user, show user-identity, show dns**, **clear configure user-identity**, **clear dns, debug user-identity, test aaa-server ad-agent**.
Identity NAT configurable proxy ARP and route lookup	In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was always used to determine the egress interface. You could not configure these settings. In 8.4(2) and later, the default behavior for identity NAT was changed to match the behavior of other static NAT configurations: proxy ARP is enabled, and the NAT configuration determines the egress interface (if specified) by default. You can leave these settings as is, or you can enable or disable them discretely. Note that you can now also disable proxy ARP for regular static NAT. For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: **no-proxy-arp** and **route-lookup**. The **unidirectional** keyword that was used for migrating to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. The **unidirectional** keyword is removed. We modified the following commands: **nat static** [**no-proxy-arp**] [**route-lookup**] (object network) and **nat source static** [**no-proxy-arp**] [**route-lookup**] (global).

Table 1-4 New Features for ASA Version 8.4(2) (continued)

Feature	Description
PAT pool and round robin address assignment	You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy. **Note** Currently in 8.4(2), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634). We modifed the following commands: **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] (object network) and **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] (global).
IPv6 Inspection	You can configure IPv6 inspection by configuring a service policy to selectively block IPv6 traffic based on the extension header. IPv6 packets are subjected to an early security check. The ASA always passes hop-by-hop and destination option types of extension headers while blocking router header and no next header. You can enable default IPv6 inspection or customize IPv6 inspection. By defining a policy map for IPv6 inspection you can configure the ASA to selectively drop IPv6 packets based on following types of extension headers found anywhere in the IPv6 packet: • Hop-by-Hop Options • Routing (Type 0) • Fragment • Destination Options • Authentication • Encapsulating Security Payload We modified the following commands: **policy-map type inspect ipv6, verify-header, match header, match header routing-type**, **match header routing-address count gt, match header count gt**.
Remote Access Features	
Portal Access Rules	This enhancement allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in the HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources. We modified the following command: **webvpn portal-access-rule**. *Also available in Version 8.2(5).*
Clientless support for Microsoft Outlook Web App 2010	The ASA 8.4(2) clientless SSL VPN core rewriter now supports Microsoft Outlook Web App 2010.

Table 1-4 New Features for ASA Version 8.4(2) (continued)

Feature	Description
Secure Hash Algorithm SHA-2 Support for IPsec IKEv2 Integrity and PRF	This release supports the Secure Hash Algorithm SHA-2 for increased cryptographic hashing security for IPsec/IKEv2 AnyConnect Secure Mobility Client connections to the ASA. SHA-2 includes hash functions with digests of 256, 384, or 512 bits, to meet U.S. government requirements. We modified the following commands: **integrity**, **prf, show crypto ikev2 sa detail**, **show vpn-sessiondb detail remote**.
Secure Hash Algorithm SHA-2 Support for Digital Signature over IPsec IKEv2	This release supports the use of SHA-2 compliant signature algorithms to authenticate IPsec IKEv2 VPN connections that use digital certificates, with the hash sizes SHA-256, SHA-384, and SHA-512. SHA-2 digital signature for IPsec IKEv2 connections is supported with the AnyConnect Secure Mobility Client, Version 3.0.1 or later.
Split Tunnel DNS policy for AnyConnect	This release includes a new policy pushed down to the AnyConnect Secure Mobility Client for resolving DNS addresses over split tunnels. This policy applies to VPN connections using the SSL or IPsec/IKEv2 protocol and instructs the AnyConnect client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyConnect client does not try to resolve the address through public DNS servers. By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy: tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list. We introduced the following command: **split-tunnel-all-dns**. *Also available in Version 8.2(5).*

Table 1-4 New Features for ASA Version 8.4(2) (continued)

Feature	Description
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	You can now configure the ASA to permit or deny VPN connections to mobile devices, enable or disable mobile device access on a per group bases, and gather information about connected mobile devices based on a mobile device's posture data. The following mobile platforms support this capability: AnyConnect for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Android Version 2.4.x. **Licensing Requirements** Enforcing remote access controls and gathering posture data from mobile devices requires an AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to be installed on the ASA. You receive the following functionality based on the license you install: • **AnyConnect Premium License Functionality** Enterprises that install the AnyConnect Premium license will be able to enforce DAP policies, on supported mobile devices, based on these DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device. • **AnyConnect Essentials License Functionality** Enterprises that install the AnyConnect Essentials license will be able to do the following: – Enable or disable mobile device access on a per group basis and to configure that feature using ASDM. – Display information about connected mobile devices via CLI or ASDM without having the ability to enforce DAP policies or deny or allow remote access to those mobile devices. *Also available in Version 8.2(5).*
SSL SHA-2 digital signature	You can now 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. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. We modified the following command: **show crypto ca certificate** (the Signature Algorithm field identifies the digest algorithm used when generating the signature). *Also available in Version 8.2(5).*
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	ASA supports SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients when using the L2TP/IPsec protocol. We did not modify any commands. *Also available in Version 8.2(5).*

Table 1-4 New Features for ASA Version 8.4(2) (continued)

Feature	Description
Enable/disable certificate mapping to override the group-url attribute	This feature changes the preference of a connection profile during the connection profile selection process. By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This optional feature changes the preference to a connection profile that specifies the group URL requested by the endpoint. The new option lets administrators rely on the group URL preference used by many older ASA software releases. We introduced the following command: **tunnel-group-preference**. *Also available in Version 8.2(5).*
ASA 5585-X Features	
Support for Dual SSPs for SSP-40 and SSP-60	For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). Each SSP acts as an independent device, with separate configurations and management. You can use the two SSPs as a failover pair if desired. **Note** When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled. We modified the following commands: **show module**, **show inventory**, **show environment**.
Support for the IPS SSP-10, -20, -40, and -60	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. *Also available in Version 8.2(5).*
CSC SSM Features	
CSC SSM Support	For the CSC SSM, support for the following features has been added: • HTTPS traffic redirection: URL filtering and WRS queries for incoming HTTPS connections. • Configuring global approved whitelists for incoming and outgoing SMTP and POP3 e-mail. • E-mail notification for product license renewals. We did not modify any commands.
Monitoring Features	
Smart Call-Home Anonymous Reporting	Customers can now help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device. We introduced the following commands: **call-home reporting anonymous, call-home test reporting anonymous**. *Also available in Version 8.2(5).*
IF-MIB ifAlias OID support	The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will be set to the value that has been set for the interface description. *Also available in Version 8.2(5).*
Interface Features	

Table 1-4 New Features for ASA Version 8.4(2) (continued)

Feature	Description
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interfaces; support was previously added for 10-Gigabit Ethernet interfaces in 8.2(2). We modified the following command: **flowcontrol**. *Also available in Version 8.2(5).*
Management Features	
Increased SSH security; the SSH default username is no longer supported	Starting in 8.4(2), you can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or Configuration > Device Management > Users/AAA > AAA Access > Authentication (ASDM); then define a local user by entering the **username** command (CLI) or choosing Configuration > Device Management > Users/AAA > User Accounts (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.
Unified Communications Features	
ASA-Tandberg Interoperability with H.323 Inspection	H.323 Inspection now supports uni-directional signaling for two-way video sessions. This enhancement allows H.323 Inspection of one-way video conferences supported by Tandberg video phones. Supporting uni-directional signaling allows Tandberg phones to switch video modes (close their side of an H.263 video session and reopen the session using H.264, the compression standard for high-definition video). We did not modify any commands. *Also available in Version 8.2(5).*
Routing Features	
Timeout for connections using a backup static route	When multiple static routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value. We modified the following command: **timeout floating-conn**. *Also available in Version 8.2(5).*

New Features in Version 8.4(1)

Released: January 31, 2011

Table 1-5 lists the new features for ASA Version 8.4(1).

Table 1-5 New Features for ASA Version 8.4(1)

Feature	Description
Hardware Features	
Support for the ASA 5585-X	We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10, -20, -40, and -60. **Note** Support was previously added in 8.2(3) and 8.2(4); the ASA 5585-X is not supported in 8.3(x).
No Payload Encryption hardware for export	You can purchase the ASA 5585-X with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. The ASA software senses a No Payload Encryption model, and disables the following features: • Unified Communications • VPN You can still install the Strong Encryption (3DES/AES) license for use with management connections. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL).
Remote Access Features	
L2TP/IPsec Support on Android Platforms	We now support VPN connections between Android mobile devices and ASA 5500 series devices, when using the L2TP/IPsec protocol and the native Android VPN client. Mobile devices must be using the Android 2.1, or later, operating system. *Also available in Version 8.2(5).*
UTF-8 Character Support for AnyConnect Passwords	AnyConnect 3.0 used with ASA 8.4(1), supports UTF-8 characters in passwords sent using RADIUS/MSCHAP and LDAP protocols.
IPsec VPN Connections with IKEv2	Internet Key Exchange Version 2 (IKEv2) is the latest key exchange protocol used to establish and control Internet Protocol Security (IPsec) tunnels. The ASA now supports IPsec with IKEv2 for the AnyConnect Secure Mobility Client, Version 3.0(1), for all client operating systems. On the ASA, you enable IPsec connections for users in the group policy. For the AnyConnect client, you specify the primary protocol (IPsec or SSL) for each ASA in the server list of the client profile. IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses. Site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). The Other VPN license is included in the Base license. We modified the following commands: **vpn-tunnel-protocol**, **crypto ikev2 policy**, **crypto ikev2 enable**, **crypto ipsec ikev2**, **crypto dynamic-map**, **crypto map**.

Table 1-5 New Features for ASA Version 8.4(1) (continued)

Feature	Description
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.
SCEP Proxy	SCEP Proxy provides the AnyConnect Secure Mobility Client with support for automated third-party certificate enrollment. Use this feature to support AnyConnect with zero-touch, secure deployment of device certificates to authorize endpoint connections, enforce policies that prevent access by non-corporate assets, and track corporate assets. This feature requires an AnyConnect Premium license and will not work with an Essentials license. We introduced or modified the following commands: **crypto ikev2 enable**, **scep-enrollment enable**, **scep-forwarding-url**, **debug crypto ca scep-proxy**, **secondary-username-from-certificate**, **secondary-pre-fill-username**.
Host Scan Package Support	This feature provides the necessary support for the ASA to install or upgrade a Host Scan package and enable or disable Host Scan. This package may either be a standalone Host Scan package or one that ASA extracts from an AnyConnect Next Generation package. In previous releases of AnyConnect, an endpoint's posture was determined by Cisco Secure Desktop (CSD). Host Scan was one of many features bundled in CSD. Unbundling Host Scan from CSD gives AnyConnect administrators greater freedom to update and install Host Scan separately from the other features of CSD. We introduced the following command: **csd hostscan image path**.
Kerberos Constrained Delegation (KCD)	This release implements the KCD protocol transition and constrained delegation extensions on the ASA. KCD provides Clientless SSL VPN (also known as WebVPN) users with SSO access to any web services protected by Kerberos. Examples of such services or applications include Outlook Web Access (OWA), Sharepoint, and Internet Information Server (IIS). Implementing protocol transition allows the ASA to obtain Kerberos service tickets on behalf of remote access users without requiring them to authenticate to the KDC (through Kerberos). Instead, a user authenticates to ASA using any of the supported authentication mechanisms, including digital certificates and Smartcards, for Clientless SSL VPN (also known as WebVPN). When user authentication is complete, the ASA requests and obtains an impersonate ticket, which is a service ticket for ASA on behalf of the user. The ASA may then use the impersonate ticket to obtain other service tickets for the remote access user. Constrained delegation provides a way for domain administrators to limit the network resources that a service trusted for delegation (for example, the ASA) can access. This task is accomplished by configuring the account under which the service is running to be trusted for delegation to a specific instance of a service running on a specific computer. We modified the following commands: **kcd-server**, **clear aaa**, **show aaa**, **test aaa-server authentication**.
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Apple Safari 5.

Table 1-5 New Features for ASA Version 8.4(1) (continued)

Feature	Description
Clientless VPN Auto Sign-on Enhancement	Smart tunnel now supports HTTP-based auto sign-on on Firefox as well as Internet Explorer. Similar to when Internet Explorer is used, the administrator decides to which hosts a Firefox browser will automatically send credentials. For some authentication methods, if may be necessary for the administrator to specify a realm string on the ASA to match that on the web application (in the Add Smart Tunnel Auto Sign-on Server window). You can now use bookmarks with macro substitutions for auto sign-on with Smart tunnel as well. The POST plug-in is now obsolete. The former POST plug-in was created so that administrators could specify a bookmark with sign-on macros and receive a kick-off page to load prior to posting the the POST request. The POST plug-in approach allows requests that required the presence of cookies, and other header items, fetched ahead of time to go through. The administrator can now specify pre-load pages when creating bookmarks to achieve the same functionality. Same as the POST plug-in, the administrator specifies the pre-load page URL and the URL to send the POST request to. You can now replace the default preconfigured SSL VPN portal with your own portal. The administrators do this by specifying a URL as an External Portal. Unlike the group-policy home page, the External Portal supports POST requests with macro substitution (for auto sign-on) as well as pre-load pages. We introduced or modified the following command: **smart-tunnel auto-signon**.
Expanded Smart Tunnel application support	Smart Tunnel adds support for the following applications: • Microsoft Outlook Exchange Server 2010 (native support). Users can now use Smart Tunnel to connect Microsoft Office Outlook to a Microsoft Exchange Server. • Microsoft Sharepoint/Office 2010. Users can now perform remote file editing using Microsoft Office 2010 Applications and Microsoft Sharepoint by using Smart Tunnel.
Interface Features	
EtherChannel support (ASA 5510 and higher)	You can configure up to 48 802.3ad EtherChannels of eight active interfaces each. **Note** You cannot use interfaces on the 4GE SSM, including the integrated 4GE SSM in slot 1 on the ASA 5550, as part of an EtherChannel. We introduced the following commands: **channel-group**, **lacp port-priority**, **interface port-channel**, **lacp max-bundle**, **port-channel min-bundle**, **port-channel load-balance**, **lacp system-priority**, **clear lacp counters**, **show lacp**, **show port-channel**.

Table 1-5 New Features for ASA Version 8.4(1) (continued)

Feature	Description
Bridge groups for transparent mode	If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups. You can configure up to 8 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group. **Note** Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group. We introduced the following commands: **interface bvi**, **bridge-group**, **show bridge-group**.
Scalability Features	
Increased contexts for the ASA 5550, 5580, and 5585-X	For the ASA 5550 and ASA 5585-X with SSP-10, the maximum contexts was increased from 50 to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was increased from 50 to 250.
Increased VLANs for the ASA 5580 and 5585-X	For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.
Additional platform support	Google Chrome has been added as a supported platform for ASA Version 8.4. Both 32-bit and 64-bit platforms are supported on Windows XP, Vista, and 7 and Mac OS X Version 6.0.
Increased connections for the ASA 5580 and 5585-X	We increased the firewall connection limits: • ASA 5580-20—1,000,000 to 2,000,000. • ASA 5580-40—2,000,000 to 4,000,000. • ASA 5585-X with SSP-10: 750,000 to 1,000,000. • ASA 5585-X with SSP-20: 1,000,000 to 2,000,000. • ASA 5585-X with SSP-40: 2,000,000 to 4,000,000. • ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.
Increased AnyConnect VPN sessions for the ASA 5580	The AnyConnect VPN session limit was increased from 5,000 to 10,000.
Increased Other VPN sessions for the ASA 5580	The other VPN session limit was increased from 5,000 to 10,000.
High Availability Features	
Stateful Failover with Dynamic Routing Protocols	Routes that are learned through dynamic routing protocols (such as OSPF and EIGRP) on the active unit are now maintained in a Routing Information Base (RIB) table on the standby unit. Upon a failover event, traffic on the secondary active unit now passes with minimal disruption because routes are known. Routes are synchronized only for link-up or link-down events on an active unit. If the link goes up or down on the standby unit, dynamic routes sent from the active unit may be lost. This is normal, expected behavior. We modified the following commands: **show failover**, **show route**, **show route failover**.
Unified Communication Features	

Table 1-5 New Features for ASA Version 8.4(1) (continued)

Feature	Description
UC Protocol Inspection Enhancements	SIP Inspection and SCCP Inspection are enhanced to support new features in the Unified Communications Solutions; such as, SCCP v2.0 support, support for GETPORT messages in SCCP Inspection, SDP field support in INVITE messages with SIP Inspection, and QSIG tunneling over SIP. Additionally, the Cisco Intercompany Media Engine supports Cisco RT Lite phones and third-party video endpoints (such as, Tandberg). We did not modify any commands.
Inspection Features	
DCERPC Enhancement	DCERPC Inspection was enhanced to support inspection of RemoteCreateInstance RPC messages. We did not modify an commands.
Troubleshooting and Monitoring Features	
SNMP traps and MIBs	Supports the following additional keywords: **connection-limit-reached**, **entity cpu-temperature**, **cpu threshold rising**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. The entPhysicalTable reports entries for sensors, fans, power supplies, and related components. Supports the following additional MIBs: ENTITY-SENSOR-MIB, CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, NAT-MIB, EVENT-MIB, EXPRESSION-MIB Supports the following additional traps: warmstart, cpmCPURisingThreshold, mteTriggerFired, cirResourceLimitReached, natPacketDiscard, ciscoEntSensorExtThresholdNotification. We introduced or modified the following commands: **snmp cpu threshold rising**, **snmp interface threshold**, **snmp-server enable traps**.
TCP Ping Enhancement	TCP ping allows users whose ICMP echo requests are blocked to check connectivity over TCP. With the TCP ping enhancement you can specify a source IP address and a port and source interface to send pings to a hostname or an IPv4 address. We modified the following command: **ping tcp**.
Show Top CPU Processes	You can now monitor the processes that run on the CPU to obtain information related to the percentage of the CPU used by any given process. You can also see information about the load on the CPU, broken down per process, at 5 minutes, 1 minute, and 5 seconds prior to the log time. Information is updated automatically every 5 seconds to provide real-time statistics, and a refresh button in the pane allows a manual data refresh at any time. We introduced the following command: **show process cpu-usage sorted**.

Table 1-5 New Features for ASA Version 8.4(1) (continued)

Feature	Description
General Features	
Password Encryption Visibility	You can show password encryption in a security context. We modified the following command: **show password encryption**.

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 ASA 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 1-23
- Firewall Mode Overview, page 1-26
- Stateful Inspection Overview, page 1-26

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the ASA 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 1-24
- Applying NAT, page 1-24
- Protecting from IP Fragments, page 1-24
- Using AAA for Through Traffic, page 1-24
- Applying HTTP, HTTPS, or FTP Filtering, page 1-24
- Applying Application Inspection, page 1-24
- Sending Traffic to the IPS Module, page 1-25

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 ASA 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 ASA. 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 ASA 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 ASA 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 ASA to perform a deep packet inspection.

Sending Traffic to the IPS Module

If your model supports the IPS module for intrusion prevention, then you can send traffic to the module for inspection. The IPS module 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 the documentation for your IPS module.

Sending Traffic to the Content Security and Control 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 ASA 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 ASA 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 ASA 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 ASA 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 is 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 ASA runs in two different firewall modes:

- Routed
- Transparent

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

In transparent mode, the ASA acts like a "bump in the wire," or a "stealth firewall," and is not considered a router hop. The ASA 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 ASA 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 53-3.

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

- Is this a new connection?

If it is a new connection, the ASA 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"

The ASA creates forward and reverse flows in the fast path for TCP traffic; the ASA also creates connection state information for connectionless protocols like UDP, ICMP (when you enable ICMP inspection), so that they can also use the fast path.

Note For other IP protocols, like SCTP, the ASA does not create reverse path flows. As a result, ICMP error packets that refer to these connections are dropped.

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 ASA 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

  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 ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA 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 ASA invokes various standard protocols to accomplish these functions.

The ASA 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 ASA invokes various standard protocols to accomplish these functions.

Security Context Overview

You can partition a single ASA 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 ASA 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 ASA. 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.