Introduction to the Cisco ASA

Released: December 3, 2012
Updated: March 31, 2014

The Cisco ASA provides advanced stateful firewall and VPN concentrator functionality in one device, and for some models, integrated services modules such as IPS. The ASA includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), clustering (combining multiple firewalls into a single firewall), 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:

- Hardware and Software Compatibility, page 1-1
- VPN Compatibility, page 1-1
- New Features, page 1-2
- Firewall Functional Overview, page 1-14
- VPN Functional Overview, page 1-18
- Security Context Overview, page 1-19
- ASA Clustering Overview, page 1-19

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 Compatibility

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

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

New Features

- New Features in ASA 9.1(5), page 1-2
- New Features in ASA 9.1(4), page 1-3
- New Features in ASA 9.1(3), page 1-5
- New Features in ASA 9.1(2), page 1-7
- New Features in ASA 9.1(1), page 1-13

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

New Features in ASA 9.1(5)

Released: March 31, 2014

Table 1-1 lists the new features for ASA Version 9.1(5).

Table 1-1 New Features for ASA Version 9.1(5)

Feature	Description
Administrative Features	
Secure Copy client	The ASA now supports the Secure Copy (SCP) client to transfer files to and from a SCP server. We introduced the following commands: **ssh pubkey-chain**, **server (ssh pubkey-chain)**, **key-string**, **key-hash**, **ssh stricthostkeycheck**. We modified the following command: **copy scp**.
Improved one-time password authentication	Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once. The **auto-enable** option was added to the **aaa authorization exec** command. We modified the following command: **aaa authorization exec**.
Firewall Features	
Transactional Commit Model on rule engine for access groups	When enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. We introduced the following comands: **asp rule-engine transactional-commit**, **show running-config asp rule-engine transactional-commit**, **clear configure asp rule-engine transactional-commit**.
Monitoring Features	

Table 1-1 New Features for ASA Version 9.1(5) (continued)

Feature	Description
SNMP hosts, host groups, and user lists	You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host. We introduced or modified the following commands: **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.
Remote Access Features	
AnyConnect DTLS Single session Performance Improvement	UDP traffic, such as streaming media, was being affected by a high number of dropped packets when sent over an AnyConnect DTLS connection. For example, this could result in streaming video playing poorly or cease streaming completely. The reason for this was the relatively small size of the flow control queue. We increased the DTLS flow-control queue size and offset this by reducing the admin crypto queue size. For TLS sessions, the priority of the crypto command was increased to high to compensated for this change. For both DTLS and TLS sessions, the session will now persist even if packets are dropped. This will prevent media streams from closing and ensure that the number of dropped packets is comparable with other connection methods. We did not modify any commands.
Webtype ACL enhancements	We introduced URL normalization. URL normalization is an additional security feature that includes path normalization, case normalization and scheme normalization. URLs specified in an ACE and portal address bar are normalized before comparison; for making decisions on webvpn traffic filtering. We did not modify any commands.

New Features in ASA 9.1(4)

Released: December 9, 2013

Table 1-2 lists the new features for ASA Version 9.1(4).

Table 1-2 New Features for ASA Version 9.1(4)

Feature	Description
Remote Access Features	
HTML5 WebSocket proxying	HTML5 WebSockets provide persistent connections between clients and servers. During the establishment of the clientless SSL VPN connection, the handshake appears to the server as an HTTP Upgrade request. The ASA will now proxy this request to the backend and provide a relay after the handshake is complete. Gateway mode is not currently supported. We did not modify any commands.

Table 1-2 New Features for ASA Version 9.1(4) (continued)

Feature	Description
Inner IPv6 for IKEv2	IPv6 traffic can now be tunneled through IPsec/IKEv2 tunnels. This makes the ASA to AnyConnect VPN connections fully IPv6 compliant. GRE is used when both IPv4 and IPv6 traffic are being tunneled, and when both the client and headend support GRE. For a single traffic type, or when GRE is not supported by the client or the headend, we use straight IPsec. **Note** This feature requires AnyConnect Client Version 3.1.05 or later. Output of the **show ipsec sa** and **show vpn-sessiondb detail anyconnect** commands has been updated to reflect the assigned IPv6 address, and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic. The **vpn-filter** command must now be used for both IPv4 and IPv6 ACLs. If the depracated **ipv6-vpn-filter** command is used to configure IPv6 ACLs the connection will be terminated.
Mobile Devices running Citrix Server Mobile have additional connection options	Support for mobile devices connecting to Citrix server through the ASA now includes selection of a tunnel-group, and RSA Securid for authorization. Allowing mobile users to select different tunnel-groups allows the administrator to use different authentication methods. We introduced the **application-type** command to configure the default tunnel group for VDI connections when a Citrix Receiver user does not choose a tunnel-group. A **none** action was added to the **vdi** command to disable VDI configuration for a particular group policy or user.
Split-tunneling supports exclude ACLs	Split-tunneling of VPN traffic has been enhanced to support both exclude and include ACLs. Exclude ACLs were previously ignored. **Note** This feature requires AnyConnect Client Version 3.1.03103 or later. We did not modify any commands.
High Availability and Scalability Features	
ASA 5500-X support for clustering	The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now support 2-unit clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 5512-X, you need the Security Plus license. We did not modify any commands.
Improved VSS and vPC support for health check monitoring	If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, you can now increase stability with health check monitoring. For some switches, such as the Nexus 5000, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable the VSS/vPC health check feature, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them. We modified the following command: **health-check** [**vss-enabled**]

Table 1-2 New Features for ASA Version 9.1(4) (continued)

Feature	Description
Support for cluster members at different geographical locations (inter-site); Individual Interface mode only	You can now place cluster members at different geographical locations when using individual interface mode. See the configuration guide for inter-site guidelines. We did not modify any commands.
Support for clustering with the Cisco Nexus 5000 and Cisco Catalyst 3750-X	The ASA supports clustering when connected to the Cisco Nexus 5000 and Cisco Catalyst 3750-X. We modified the following command: **health-check** [**vss-enabled**]
Basic Operation Features	
DHCP rebind function	During the DHCP rebind phase, the client now attempts to rebind to other DHCP servers in the tunnel group list. Prior to this release, the client did not rebind to an alternate server, when the DHCP lease fails to renew. We introduced the following commands: **show ip address dhcp lease proxy**, **show ip address dhcp lease summary**, and **show ip address dhcp lease server**.
Troubleshooting Features	
Crashinfo dumps include AK47 framework information	Application Kernel Layer 4 to 7 (AK47) framework-related information is now available in crashinfo dumps. A new option, **ak47**, has been added to the **debug menu** command to help in debugging AK47 framework issues. The framework-related information in the crashinfo dump includes the following: • Creating an AK47 instance. • Destroying an AK47 instance. • Generating an crashinfo with a memory manager frame. • Generating a crashinfo after fiber stack overflow. • Generating a crashinfo after a local variable overflow. • Generating a crashinfo after an exception has occurred.

New Features in ASA 9.1(3)

Released: September 18, 2013

Table 1-3 lists the new features for ASA Version 9.1(3).

Table 1-3 New Features for ASA Version 9.1(3)

Feature	Description
Module Features	
Support for the ASA CX module in multiple context mode	You can now configure ASA CX service policies per context on the ASA. **Note** Although you can configure per context ASA service policies, the ASA CX module itself (configured in PRSM) is a single context mode device; the context-specific traffic coming from the ASA is checked against the common ASA CX policy. Requires ASA CX 9.2(1) or later. We did not modify any commands.
ASA 5585-X with SSP-40 and -60 support for the ASA CX SSP-40 and -60	ASA CX SSP-40 and -60 modules can be used with the matching level ASA 5585-X with SSP-40 and -60. Requires ASA CX 9.2(1) or later. We did not modify any commands.
Filtering packets captured on the ASA CX backplane	You can now filter packets that have been captured on the ASA CX backplane using the **match** or **access-list** keyword with the **capture interface asa_dataplane** command. Control traffic specific to the ASA CX module is not affected by the access-list or match filtering; the ASA captures all control traffic. In multiple context mode, configure the packet capture per context. Note that all control traffic in multiple context mode goes only to the system execution space. Because only control traffic cannot be filtered using an access list or match, these options are not available in the system execution space. Requires ASA CX 9.2(1) or later. We modified the following command: **capture interface asa_dataplane**.
Monitoring Features	
Ability to view top 10 memory users	You can now view the top bin sizes allocated and the top 10 PCs for each allocated bin size. Previously, you had to enter multiple commands to see this information (the **show memory detail** command and the **show memory binsize** command); the new command provides for quicker analysis of memory issues. We introduced the following command: **show memory top-usage**. *Also available in 8.4(6).*

Table 1-3 New Features for ASA Version 9.1(3) (continued)

Feature	Description
Smart Call Home	We added a new type of Smart Call Home message to support ASA clustering. A Smart Call Home clustering message is sent for only the following three events: • When a unit joins the cluster • When a unit leaves the cluster • When a cluster unit becomes the cluster master Each message that is sent includes the following information: • The active cluster member count • The output of the **show cluster info** command and the **show cluster history** command on the cluster master We modified the following commands: **show call-home, show running-config call-home**. *Also available in 9.0(3).*
Remote Access Features	
user-storage value command password is now encrypted in **show** commands	The password in the **user-storage value** command is now encrypted when you enter **show running-config**. We modified the following command: **user-storage value**. *Also available in 8.4(6).*

New Features in ASA 9.1(2)

Released: May 14, 2013

Table 1-4 lists the new features for ASA Version 9.1(2).

Note Features added in 8.4(6) are not included in 9.1(2) unless they are explicitly listed in this table.

Table 1-4 New Features for ASA Version 9.1(2)

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 series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X, and the ASA Services Module. 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.
Encryption Features	

Table 1-4 New Features for ASA Version 9.1(2) (continued)

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications</td><td>
Instead of using the proprietary encryption for the failover key (the failover key command), you can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption.
Note Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.
We introduced or modified the following commands: failover ipsec pre-shared-key, show vpn-sessiondb.
</td></tr>
<tr><td>Additional ephemeral Diffie-Hellman ciphers for SSL encryption</td><td>
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.
<pre>!! set server version
hostname(config)# ssl server-version tlsv1 sslv3
!! set client version
hostname(config) # ssl client-version any</pre>
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.
Also available in 8.4(4.1).
</td></tr>
<tr><td colspan="2">Management Features</td></tr>
<tr><td>Support for administrator password policy when using the local database</td><td>
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 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.
Also available in 8.4(4.1).
</td></tr>
</table>

Table 1-4 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Support for SSH public key authentication	You can now enable public key authentication for SSH connections to the ASA on a per-user basis. You can specify a public key file (PKF) formatted key or a Base64 key. The PKF key can be up to 4096 bits. Use PKF format for keys that are too large to for the ASA support of the Base64 format (up to 2048 bits). We introduced the following commands: **ssh authentication**. *Also available in 8.4(4.1); PKF key format support is only in 9.1(2).*
AES-CTR encryption for SSH	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
Improved SSH rekey interval	An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic. We introduced the following command: **show ssh sessions detail**.
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**. *Also available in 8.4(4.1).*
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**. *Also available in 8.4(4.1).*
The default Telnet password was removed	To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication (the **aaa authentication telnet console** command). Formerly, when you cleared the password, the ASA restored the default of "cisco." Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASASM (see the **session** command). For initial ASASM access, you must use the **service-module session** command, until you set a login password. We modified the following command: **passwd**. *Also available in 9.0(2).*
Platform Features	
Support for Power-On Self-Test (POST)	The ASA runs its power-on self-test at boot time even if it is not running in FIPS 140-2-compliant mode. Additional tests have been added to the POST to address the changes in the AES-GCM/GMAC algorithms, ECDSA algorithms, PRNG, and Deterministic Random Bit Generator Validation System (DRBGVS).
Improved pseudo-random number generation (PRNG)	The X9.31 implementation has been upgraded to use AES-256 encryption instead of 3DES encryption to comply with the Network Device Protection Profile (NDPP) in single-core ASAs.
Support for image verification	Support for SHA-512 image integrity checking was added. We modified the following command: **verify**. *Also available in 8.4(4.1).*

Table 1-4 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Support for private VLANs on the ASA Services Module	You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information.
CPU profile enhancements	The **cpu profile activate** command now supports the following: • Delayed start of the profiler until triggered (global or specific thread CPU%) • Sampling of a single thread We modified the following command: **cpu profile activate** [*n-samples*] [**sample-process** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*]. *Also available in 8.4(6).*
DHCP Features	
DHCP relay servers per interface (IPv4 only)	You can now configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. IPv6 is not supported for per-interface DHCP relay. We introduced or modified the following commands: **dhcprelay server** (interface config mode), **clear configure dhcprelay**, **show running-config dhcprelay**.
DHCP trusted interfaces	You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface. We introduced or modified the following commands: **dhcprelay information trusted**, **dhcprelay informarion trust-all**, **show running-config dhcprelay**.
Module Features	
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 *Also available in 8.4(4.1).*
ASA 5585-X DC power supply support	Support was added for the ASA 5585-X DC power supply. *Also available in 8.4(5).*

Table 1-4 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Support for ASA CX monitor-only mode for demonstration purposes	For demonstration purposes only, you can enable monitor-only mode for the service policy, which forwards a copy of traffic to the ASA CX module, while the original traffic remains unaffected. Another option for demonstration purposes is to configure a traffic-forwarding interface instead of a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic directly to the ASA CX module, bypassing the ASA. We modified or introduced the following commands: **cxsc** {**fail-close** | **fail-open**} **monitor-only**, **traffic-forward cxsc monitor-only**.
Support for the ASA CX module and NAT 64	You can now use NAT 64 in conjunction with the ASA CX module. We did not modify any commands.
NetFlow Features	
Support for NetFlow flow-update events and an expanded set of NetFlow templates	In addition to adding the flow-update events, there are now NetFlow templates that allow you to track flows that experience a change to their IP version with NAT, as well as IPv6 flows that remain IPv6 after NAT. Two new fields were added for IPv6 translation support. Several NetFlow field IDs were changed to their IPFIX equivalents. For more information, see the *Cisco ASA Implementation Note for NetFlow Collectors*.
Firewall Features	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL. We modified the following command: **access-list ethertype** {**permit** | **deny**} **is-is**. *Also available in 8.4(5).*
Decreased the half-closed timeout minimum value to 30 seconds	The half-closed timeout minimum value for both the global timeout and connection timeout was lowered from 5 minutes to 30 seconds to provide better DoS protection. We modified the following commands: **set connection timeout half-closed**, **timeout half-closed**.
Remote Access Features	

Table 1-4 New Features for ASA Version 9.1(2) (continued)

Feature	Description
IKE security and performance improvements	The number of IPsec-IKE security associations (SAs) can be limited for IKE v1 now, as well as IKE v2. We modified the following command: **crypto ikev1 limit**.
	The IKE v2 Nonce size has been increased to 64 bytes. There are no ASDM screen or CLI changes.
	For IKE v2 on Site-to-Site, a new algorithm ensures that the encryption algorithm used by child IPsec SAs is not higher strength than the parent IKE. Higher strength algorithms will be downgraded to the IKE level. This new algorithm is enabled by default. We recommend that you do not disable this feature. We introduced the following command: **crypto ipsec ikev2 sa-strength-enforcement**.
	For Site-to-Site, IPsec data-based rekeying can be disabled. We modified the following command: **crypto ipsec security-association**.
Improved Host Scan and ASA Interoperability	Host Scan and the ASA use an improved process to transfer posture attributes from the client to the ASA. This gives the ASA more time to establish a VPN connection with the client and apply a dynamic access policy. *Also available in 8.4(5).*
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems. We support the following browsers on Windows 8: • Internet Explorer 10 (desktop only) • Firefox (all supported Windows 8 versions) • Chrome (all supported Windows 8 versions) See the following limitations: • Internet Explorer 10: – The Modern (AKA Metro) browser is not supported. – If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone. – If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported. • A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported. *Also available in 9.0(2).*

Table 1-4 New Features for ASA Version 9.1(2) (continued)

Feature	Description
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check. See the following limitations: • Secure Desktop (Vault) is not supported with Windows 8. *Also available in 9.0(2).*
Monitoring Features	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the **show xlate count** command. *Also available in 8.4(5).*
NSEL	Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent. We introduced or modified the following commands: **flow-export active refresh-interval**, **flow-export event-type**. *Also available in 8.4(5).*

New Features in ASA 9.1(1)

Released: December 3, 2012

Table 1-5 lists the new features for ASA Version 9.1(1).

Note Features added in 8.4(4.x), 8.4(5), 8.4(6), and 9.0(2) are not included in 9.1(1) unless they were listed in the 9.0(1) feature table.

Table 1-5 New Features for ASA Version 9.1(1)

Feature	Description
Module Features	
Support for the ASA CX SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA CX SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. The ASA CX software module requires a Cisco solid state drive (SSD) on the ASA. For more information about the SSD, see the ASA 5500-X hardware guide. We modified the following commands: **session cxsc**, **show module cxsc**, **sw-module cxsc**.

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 1-14
- Firewall Mode Overview, page 1-17
- Stateful Inspection Overview, page 1-17

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 1-15
- Applying NAT, page 1-15
- Protecting from IP Fragments, page 1-15
- Using AAA for Through Traffic, page 1-15
- Applying HTTP, HTTPS, or FTP Filtering, page 1-15
- Applying Application Inspection, page 1-15
- Sending Traffic to a Module, page 1-15
- Applying QoS Policies, page 1-16
- Applying Connection Limits and TCP Normalization, page 1-16
- Enabling Threat Detection, page 1-16
- Enabling the Botnet Traffic Filter, page 1-16
- Configuring Cisco Unified Communications, page 1-16

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 consider using Cisco Web Security Appliance, a dedicated web proxy that provides advanced web filtering as well as advanced threat defense, advanced malware protection, application visibility and control, insightful reporting, and secure mobility. For additional information, see http://www.cisco.com/go/websecurity.

You may also the ASA in conjunction with a third-party server running a filtering product such as Websense Enterprise.

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 do a deep packet inspection.

Sending Traffic to a Module

If your model supports an add-on module, then you can send traffic to the module for inspection. For more information, see the documentation for your module.

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 in the firewall configuration guide.

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.

ASA Clustering Overview

ASA Clustering lets you group multiple ASAs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

You perform all configuration (aside from the bootstrap configuration) on the master unit only; the configuration is then replicated to the member units.