Introduction to the Cisco ASA

The Cisco ASA provides advanced stateful firewall and VPN concentrator functionality in one device as well as integrated services with add-on modules. 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.

- Hardware and Software Compatibility, on page 1
- VPN Compatibility, on page 1
- New Features, on page 1
- Firewall Functional Overview, on page 10
- VPN Functional Overview, on page 14
- Security Context Overview, on page 14
- ASA Clustering Overview, on page 15
- Special and Legacy Services, on page 15

Hardware and Software Compatibility

For a complete list of supported hardware and software, see Cisco ASA Compatibility.

VPN Compatibility

See Supported VPN Platforms, Cisco ASA Series.

New Features

This section lists new features for each release.

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

New Features in ASA 9.13(1)

Released: September 25, 2019

Feature	Description
Platform Features	
ASA for the Firepower 1010	We introduced the ASA for the Firepower 1010. This desktop model includes a built-in hardware switch and Power-Over-Ethernet+ (PoE+) support. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **forward interface**, **interface vlan**, **power inline**, **show counters**, **show environment**, **show interface**, **show inventory**, **show power inline**, **show switch mac-address-table**, **show switch vlan**, **switchport**, **switchport access vlan**, **switchport mode**, **switchport trunk allowed vlan**
ASA for the Firepower 1120, 1140, and 1150	We introduced the ASA for the Firepower 1120, 1140, and 1150. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **show counters**, **show environment**, **show interface**, **show inventory**
Firepower 2100 Appliance mode	The Firepower 2100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). You can run the Firepower 2100 in the following modes: • Appliance mode (now the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI. • Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Firepower Chassis Manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI. If you are upgrading to 9.13(1), the mode will remain in Platform mode. New/Modified commands: **boot system**, **clock timezone**, **connect fxos admin**, **fxos mode appliance**, **show counters**, **show environment**, **show fxos mode**, **show interface**, **show inventory**
DHCP reservation	The ASA DHCP server now supports DHCP reservation. You can assign a static IP address from the defined address pool to a DHCP client based on the client's MAC address. New/Modified commands: **dhcpd reserve-address**
ASAv minimum memory requirement	The minimum memory requirement for the ASAv is now 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version without increasing the memory of your ASAv VM. You can also redeploy a new ASAv VM with version 9.13(1). No modified commands.

Feature	Description
ASAv MSLA Support	The ASAv supports Cisco's Managed Service License Agreement (MSLA) program, which is a software licensing and consumption framework designed for Cisco customers and partners who offer managed software services to third parties. MSLA is a new form of Smart Licensing where the licensing Smart Agent keeps track of the usage of licensing entitlements in units of time. New/Modified commands: **license smart**, **mode**, **utility**, **custom-id**, **custom-info**, **privacy**, **transport type**, **transport url**, **transport proxy**
ASAv Flexible Licensing	Flexible Licensing is a new form of Smart Licensing where any ASAv license now can be used on any supported ASAv vCPU/memory configuration. Session limits for AnyConnect and TLS proxy will be determined by the ASAv platform entitlement installed rather than a platform limit tied to a model type. New/Modified commands: **show version**, **show vm**, **show cpu**, **show license features**
ASAv for AWS support for the C5 instance; expanded support for C4, C3, and M4 instances	The ASAv on the AWS Public Cloud now supports the C5 instance (c5.large, c5.xlarge, and c5.2xlarge). In addition, support has been expanded for the C4 instance (c4.2xlarge and c4.4xlarge); C3 instance (c3.2xlarge, c3.4xlarge, and c3.8xlarge); and M4 instance (m4.2xlarge and m4.4xlarge). No modified commands.
ASAv for Microsoft Azure support for more Azure virtual machine sizes	The ASAv on the Microsoft Azure Public Cloud now supports more Linux virtual machine sizes: • Standard_D4, Standard_D4_v2 • Standard_D8_v3 • Standard_DS3, Standard_DS3_v2 • Standard_DS4, Standard_DS4_v2 • Standard_F4, Standard_F4s • Standard_F8, Standard_F8s Earlier releases only supported the Standard_D3 and Standard_D3_v2 sizes. No modified commands.
ASAv enhanced support for DPDK	The ASAv supports enhancements to the Data Plane Development Kit (DPDK) to enable support for multiple NIC queues, which allow multi-core CPUs to concurrently and efficiently service network interfaces. This applies to all ASAv hypervisors except Microsoft Azure and Hyper-V. **Note** DPDK support was introduced in release ASA 9.10(1). No modified commands.

Feature	Description
ASAv support for VMware ESXi 6.7	The ASAv virtual platform supports hosts running on VMware ESXi 6.7. New VMware hardware versions have been added to the *vi.ovf* and *esxi.ovf* files to enable optimal performance and usability of the ASAv on ESXi 6.7. No modified commands.
Increased VLANs for the ISA 3000	The maximum VLANs for the ISA 3000 with the Security Plus license increased from 25 to 100.
Firewall Features	
Location logging for mobile stations (GTP inspection).	You can configure GTP inspection to log the initial location of a mobile station and subsequent changes to the location. Tracking location changes can help you identify possibly fraudulent roaming charges. New/Modified commands: **location-logging**.
GTPv2 and GTPv1 release 15 support.	The system now supports GTPv2 3GPP 29.274 V15.5.0. For GTPv1, support is up to 3GPP 29.060 V15.2.0. The new support includes recognition of 2 additional messages and 53 information elements. No modified commands.
Mapping Address and Port-Translation (MAP-T)	Mapping Address and Port (MAP) is primarily a feature for use in service provider (SP) networks. The service provider can operate an IPv6-only network, the MAP domain, while supporting IPv4-only subscribers and their need to communicate with IPv4-only sites on the public Internet. MAP is defined in RFC7597, RFC7598, and RFC7599. New/Modified commands: **basic-mapping-rule**, **default-mapping-rule**, **ipv4-prefix**, **ipv6-prefix**, **map-domain**, **share-ratio**, **show map-domain**, **start-port**.
Increased limits for AAA server groups and servers per group.	You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4). In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged. We modified the following commands to accept these new limits: **aaa-server**, **aaa-server host**.
TLS proxy deprecated for SCCP (Skinny) inspection.	The **tls-proxy** keyword, and support for SCCP/Skinny encrypted inspection, was deprecated. The keyword will be removed from the **inspect skinny** command in a future release.
VPN Features	

Feature	Description
HSTS Support for WebVPN as Client	A new CLI mode under WebVPN mode called http-headers was added so that WebVPN could transform HTTP references to HTTPS references for hosts that are HSTS. Configures whether the user agent should allow the embedding of resources when sending this header for WebVPN connections from the ASA to browsers. You can choose to configure the http-headers as: **x-content-type-options**, **x-xss-protection**, **hsts-client** (HSTS support for WebVPN as client), **hsts-server**, or **content-security-policy**. New/Modified commands: **webvpn**, **show webvpn hsts host (name <hostname&s{253}> | all)**and **clear webvpn hsts host (name <hostname&s{253}> | all)**.
Diffie-Hellman groups 15 and 16 added for key exchange	To add support for Diffie-Hellman groups 15 and 16, we modified few **crypto** commands to accept these new limits. **crypto ikev2 policy <index> group <number>** and **crypto map <map-name> <map-index> set pfs <group>.**
show asp table vpn-context enhancement to output	To enhance debug capability, these vpn context counters were added to the output: Lock Err, No SA, IP Ver Err, and Tun Down. New/Modified commands: **show asp table vpn-context** (output only).
Immediate session establishment when the maximum remote access VPN session limit is reached.	When a user reaches the maximum session (login) limit, the system deletes the user's oldest session and waits for the deletion to complete before establishing the new session. This can prevent the user from successfully connecting on the first attempt. You can remove this delay and have the system establish the new connection without waiting for the deletion to complete. New/Modified commands: **vpn-simultaneous-login-delete-no-delay**.
High Availability and Scalability Features	
Initiator and responder information for Dead Connection Detection (DCD), and DCD support in a cluster.	If you enable Dead Connection Detection (DCD), you can use the **show conn detail** command to get information about the initiator and responder. Dead Connection Detection allows you to maintain an inactive connection, and the **show conn** output tells you how often the endpoints have been probed. In addition, DCD is now supported in a cluster. New/Modified commands: **show conn** (output only).
Monitor the traffic load for a cluster	You can now monitor the traffic load for cluster members, including total connection count, CPU and memory usage, and buffer drops. If the load is too high, you can choose to manually disable clustering on the unit if the remaining units can handle the load, or adjust the load balancing on the external switch. This feature is enabled by default. New/Modified commands: **debug cluster load-monitor**, **load-monitor**, **show cluster info load-monitor**

Feature	Description
Accelerated cluster joining	When a data unit has the same configuration as the control unit, it will skip syncing the configuration and will join faster. This feature is enabled by default. This feature is configured on each unit, and is not replicated from the control unit to the data unit. **Note** Some configuration commands are not compatible with accelerated cluster joining; if these commands are present on the unit, even if accelerated cluster joining is enabled, configuration syncing will always occur. You must remove the incompatible configuration for accelerated cluster joining to work. Use the **show cluster info unit-join-acceleration incompatible-config** to view incompatible configuration. New/Modified commands: **unit join-acceleration**, **show cluster info unit-join-acceleration incompatible-config**
Routing Features	
SMTP configuration enhancement	You can optionally configure the SMTP server with primary and backup interface names to enable ASA for identifying the routing table to be used for logging—management routing table or data routing table. If no interface is provided, ASA would refer to management routing table lookup, and if no proper route entry is present, it would look at the data routing table. New/Modified commands: **smtp-server [primary-interface][backup-interface]**
Support to set NSF wait timer	OSPF routers are expected to set the RS-bit in the EO-TLV attached to a Hello packet when it is not known whether all neighbors are listed in the packet, and the restarting router require to preserve their adjacencies. However, the RS-bit value must not be longer than the RouterDeadInterval seconds. The **timers nsf wait**command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds. New/Modified commands: **timers nsf wait**
Support to set tftp blocksize	The typical blocksize fixed for tftp file transfer is 512-octets. A new command, **tftp blocksize**, is introduced to configure a larger blocksize and thereby enhance the tftp file transfer speed. You can set a blocksize varying from 513 to 8192 octets. The new default blocksize is 1456 octets. The **no** form of this command will reset the blocksize to the older default value—512 octets. The **timers nsf wait**command is introduced to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds. New/Modified commands: **tftp blocksize**
Certificate Features	
Support to view FIPS status	The **show running-configuration fips** command displayed the FIPS status only when fips was enabled. In order to know the operational state, the **show fips** command was introduced where, it displays the fips status when an user enables or disables fips that is in disabled or enabled state. This command also displays the status for rebooting the device after an enable or disable action. New/Modified commands: **show fips**

Feature	Description
CRL cache size increased	To prevent failure of large CRL downloads, the cache size was increased, and the limit on the number of entries in an individual CRL was removed. • Increased the total CRL cache size to 16 MB per context for multi-context mode. • Increased the total CRL cache size to 128 MB for single-context mode.
Modifications to the CRL Distribution Point commands	The static CDP URL configuration commands are removed and moved to the match certificate command. New/Modified commands: **crypto-ca-trustpoint crl** and **crl url** were removed with other related logic. **match-certificate override-cdp** was introduced. The static CDP URL was re-introduced in 9.13(1)12 to the match certificate command.
Administrative and Troubleshooting Features	
Management access when the Firepower 1000, Firepower 2100 Appliance mode is in licensing evaluation mode	The ASA includes 3DES capability by default for management access only, so you can connect to the License Authority and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have the Strong Encryption license enabled, which requires you to first register to the License Authority. **Note** If you attempt to configure any features that can use strong encryption before you have the license—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature. No modified commands.
Additional NTP authentication algorithms	Formerly, only MD5 was supported for NTP authentication. The ASA now supports the following algorithms: • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC New/Modified commands: **ntp authentication-key**
ASA Security Service Exchange (SSE) Telemetry Support for the Firepower 4100/9300	With Cisco Success Network enabled in your network, device usage information and statistics are provided to Cisco which is used to optimize technical support. The telemetry data that is collected on your ASA devices includes CPU, memory, disk, or bandwidth usage, license usage, configured feature list, cluster/failover information and the like. New/Modified commands: **service telemetry**and **show telemetry**

Feature	Description
SSH encryption ciphers are now listed in order from highest to lowest security for pre-defined lists	SSH encryption ciphers are now listed in order from highest security to lowest security for pre-defined lists (such as medium or high). In earlier releases, they were listed from lowest to highest, which meant that a low security cipher would be proposed before a high security cipher. New/Modified commands: **ssh cipher encryption**
show tech-support includes additional output	The output of **show tech-support** is enhanced to display the output of the following: **show flow-offload info detail** **show flow-offload statistics** **show asp table socket** New/Modified commands: **show tech-support** (output only).
Enhancement to **show-capture asp_drop** output to include drop location information	While troubleshooting using ASP drop counters, the exact location of the drop is unknown, especially when the same ASP drop reason is used in many different places. This information is critical in finding root cause of the drop. With this enhancement, the ASP drop details such as the build target, ASA release number, hardware model, and ASLR memory text region (to facilitate the decode of drop location) are shown. New/Modified commands: **show-capture asp_drop**
Modifications to **debug crypto ca**	The **debug crypto ca transactions** and **debug crypto ca messages** options are consolidated to provide all applicable content into the **debug crypto ca** command itself. Also, the number of available debugging levels are reduced to 14. New/Modified commands: **debug crypto ca**
FXOS Features for the Firepower 1000 and 2100	
Secure Erase	The secure erase feature erases all data on the SSDs so that data cannot be recovered even by using special tools on the SSD itself. You should perform a secure erase in FXOS when decomissioning the device. New/Modified FXOS commands: **erase secure** (local-mgmt) Supported models: Firepower 1000 and 2100
Configurable HTTPS protocol	You can set the SSL/TLS versions for FXOS HTTPS acccess. New/Modified FXOS commands: **set https access-protocols** Supported models: Firepower 2100 in Platform Mode

Feature	Description
FQDN enforcement for IPSec and Keyrings	For FXOS, you can configure FQDN enforcement so that the FDQN of the peer needs to match the DNS Name in the X.509 Certificate presented by the peer. For IPSec, enforcement is enabled by default, except for connections created prior to 9.13(1); you must manually enable enforcement for those old connections. For keyrings, all hostnames must be FQDNs, and cannot use wild cards. New/Modified FXOS commands: **set dns**, **set e-mail**, **set fqdn-enforce**, **set ip**, **set ipv6**, **set remote-address**, **set remote-ike-id** Removed commands: **fi-a-ip**, **fi-a-ipv6**, **fi-b-ip**, **fi-b-ipv6** Supported models: Firepower 2100 in Platform Mode
New IPSec ciphers and algorithms	We added the following IKE and ESP ciphers and algorithms to configure an IPSec tunnel to encrypt FXOS management traffic: • Ciphers—aes192. Existing ciphers include: aes128, aes256, aes128gcm16. • Pseudo-Random Function (PRF) (IKE only)—prfsha384, prfsha512, prfsha256. Existing PRFs include: prfsha1. • Integrity Algorithms—sha256, sha384, sha512, sha1_160. Existing algorithms incldue: sha1. • Diffie-Hellman Groups—curve25519, ecp256, ecp384, ecp521,modp3072, modp4096. Existing groups include: modp2048. No modified FXOS commands. Supported models: Firepower 2100 in Platform Mode
SSH authentication enhancements	We added the following SSH server encryption algoritghms for FXOS: • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com We added the following SSH server key exchange methods for FXOS: • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 New/Modified FXOS commands: **set ssh-server encrypt-algorithm**, **set ssh-server kex-algorithm** Supported models: Firepower 2100 in Platform Mode

Feature	Description
EDCS keys for X.509 Certificates	You can now use EDCS keys for FXOS certificates. Formerly, only RSA keys were supported. New/Modified FXOS commands: **set elliptic-curve**, **set keypair-type** Supported models: Firepower 2100 in Platform Mode
User password improvements	We added FXOS password security improvements, including the following: • User passwords can be up to 127 characters. The old limit was 80 characters. • Strong password check is enabled by default. • Prompt to set admin password. • Password expiration. • Limit password reuse. • Removed the **set change-during-interval** command, and added a **disabled** option for the **set change-interval**, **set no-change-interval**, and **set history-count** commands. New/Modified FXOS commands: **set change-during-interval**, **set expiration-grace-period**, **set expiration-warning-period**, **set history-count**, **set no-change-interval**, **set password**, **set password-expiration**, **set password-reuse-interval** Supported models: Firepower 2100 in Platform Mode

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.

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.

Permitting or Denying Traffic with Access Rules

You can apply access rules to limit traffic from inside to outside, or allow traffic from outside to inside. For bridge group interfaces, you can also apply an EtherType access rule 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.

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.

You can configure Cloud Web Security on the ASA, or install an ASA module that provides URL and other filtering services, such as ASA CX or ASA FirePOWER. You can also use the ASA in conjunction with an external product such as the Cisco Web Security Appliance (WSA).

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 Supported Hardware or Software Modules

Some ASA models allow you to configure software modules, or to insert hardware modules into the chassis, to provide advanced services. These modules provide additional traffic inspection and can block traffic based on your configured policies. You can send traffic to these modules to take advantage of these advanced services.

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.

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 in a "bridge group".

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.

Routed mode supports Integrated Routing and Bridging, so you can also configure bridge groups in routed mode, and route between bridge groups and regular interfaces. In routed mode, you can replicate transparent mode functionality; if you do not need multiple context mode or clustering, you might consider using routed mode instead.

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.

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; however, some features are not supported. See the feature chapters for more information.

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 control unit only; the configuration is then replicated to the member units.

Special and Legacy Services

For some services, documentation is located outside of the main configuration guides and online help.

Special Services Guides

Special services allow the ASA to interoperate with other Cisco products; for example, by providing a security proxy for phone services (Unified Communications), or by providing Botnet traffic filtering in conjunction with the dynamic database from the Cisco update server, or by providing WCCP services for the Cisco Web Security Appliance. Some of these special services are covered in separate guides:

- Cisco ASA Botnet Traffic Filter Guide
- Cisco ASA NetFlow Implementation Guide
- Cisco ASA Unified Communications Guide
- Cisco ASA WCCP Traffic Redirection Guide
- SNMP Version 3 Tools Implementation Guide

Legacy Services Guide

Legacy services are still supported on the ASA, however there may be better alternative services that you can use instead. Legacy services are covered in a separate guide:

Cisco ASA Legacy Feature Guide

This guide includes the following chapters:

- Configuring RIP
- AAA Rules for Network Access
- Using Protection Tools, which includes Preventing IP Spoofing (**ip verify reverse-path**), Configuring the Fragment Size (**fragment**), Blocking Unwanted Connections (**shun**), Configuring TCP Options (for ASDM), and Configuring IP Audit for Basic IPS Support (**ip audit**).
- Configuring Filtering Services