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

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 9.4(4.5)

Released: April 3, 2017

Note Verion 9.4(4) was removed from Cisco.com due to bug CSCvd78303.

There are no new features in this release.

New Features in ASA 9.4(3)

Released: April 25, 2016

Feature	Description
Firewall Features	
Connection holddown timeout for route convergence	You can now configure how long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. You can reduce the holddown timer to make route convergence happen more quickly. However, the 15 second default is appropriate for most networks to prevent route flapping. We added the following command: **timeout conn-holddown**
Remote Access Features	
Configurable SSH encryption and HMAC algorithm.	Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. We introduced the following commands: **ssh cipher encryption, ssh cipher integrity**. *Also available in 9.1(7).*
HTTP redirect support for IPv6	When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address. We added functionality to the following command: **http redirect** *Also available in 9.1(7).*
Monitoring Features	
SNMP engineID sync for Failover	In a failover pair, the SNMP engineIDs of the paired ASAs are synced on both units. Three sets of engineIDs are maintained per ASA—synced engineID, native engineID and remote engineID. An SNMPv3 user can also specify the engineID of the ASA when creating a profile to preserve localized **snmp-server user** authentication and privacy options. If a user does not specify the native engineID, the **show running config** output will show two engineIDs per user. We modified the following command: **snmp-server user**

Feature	Description
show tech support enhancements	The **show tech support** command now: • Includes **dir all-filesystems** output—This output can be helpful in the following cases: • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Removes the **show kernel cgroup-controller detail** output—This command output will remain in the output of **show tech-support detail**. We modified the following command: **show tech support** *Also available in 9.1(7).*
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now supported. This is a table of memory pool monitoring entries for all physical entities on a managed system. **Note** The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and supports reporting of memory on platforms with more than 4GB of RAM. We did not add or modify any commands. *Also available in 9.1(7).*

New Features in ASA 9.4(2.145)

Released: November 13, 2015

There are no new features in this release.

Note This release supports only the Firepower 9300 ASA security module.

New Features in ASA 9.4(2)

Released: September 24, 2015

There are no new features in this release.

Note ASAv 9.4(1.200) features are not included in this release.

Note This version does not support the ISA 3000.

New Features in ASA 9.4(1.225)

Released: September 17, 2015

Note This release supports only the Cisco ISA 3000.

Feature	Description
Platform Features	
Cisco ISA 3000 Support	The Cisco ISA 3000 is a DIN Rail mounted, ruggedized, industrial security appliance. It is low-power, fan-less, with Gigabit Ethernet and a dedicated management port. This model comes with the ASA Firepower module pre-installed. Special features for this model include a customized transparent mode default configuration, as well as a hardware bypass function to allow traffic to continue flowing through the appliance when there is a loss of power. We introduced the following commands: **hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay, show hardware-bypass** *This feature is not available in Version 9.5(1).*

New Features in ASA 9.4(1.152)

Released: July 13, 2015

Note This release supports only the ASA on the Firepower 9300.

Feature	Description
Platform Features	
ASA security module on the Firepower 9300	We introduced the ASA security module on the Firepower 9300. **Note** Firepower Chassis Manager 1.1.1 does not support any VPN features (site-to-site or remote access) for the ASA security module on the Firepower 9300.
High Availability Features	
Intra-chassis ASA Clustering for the Firepower 9300	You can cluster up to 3 security modules within the Firepower 9300 chassis. All modules in the chassis must belong to the cluster. We introduced the following commands: **cluster replication delay, debug service-module, management-only individual, show cluster chassis**
Licensing Features	

Feature	Description
Cisco Smart Software Licensing for the ASA on the Firepower 9300	We introduced Smart Software Licensing for the ASA on the Firepower 9300. We introduced the following commands: **feature strong-encryption, feature mobile-sp, feature context**

New Features in ASAv 9.4(1.200)

Released: May 12, 2015

Note This release supports only the ASAv.

Feature	Description
Platform Features	
ASAv on VMware no longer requires vCenter support	You can now install the ASAv on VMware without vCenter using the vSphere client or the OVFTool using a Day 0 configuration.
ASAv on Amazon Web Services (AWS)	You can now use the ASAv with Amazon Web Services (AWS) and the Day 0 configuration. **Note** Amazon Web Services only supports models ASAv10 and ASAv30.

New Features in ASA 9.4(1)

Released: March 30, 2015

Feature	Description
Platform Features	
ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X	We introduced the ASA 5506W-X with wireless access point, hardened ASA 5506H-X, ASA 5508-X, and ASA 5516-X models. We introduced the following command: **hw-module module wlan recover image**, **hw-module module wlan recover image**.
Certification Features	

Feature	Description
Department of Defense Unified Capabilities Requirements (UCR) 2013 Certification	The ASA was updated to comply with the DoD UCR 2013 requirements. See the rows in this table for the following features that were added for this certification: • Periodic certificate authentication • Certificate expiration alerts • Enforcement of the basic constraints CA flag • ASDM Username From Certificate Configuration • ASDM management authorization • IKEv2 invalid selectors notification configuration • IKEv2 pre-shared key in Hex
FIPS 140-2 Certification compliance updates	When you enable FIPS mode on the ASA, additional restrictions are put in place for the ASA to be FIPS 140-2 compliant. Restrictions include: • RSA and DH Key Size Restrictions—Only RSA and DH keys 2K (2048 bits) or larger are allowed. For DH, this means groups 1 (768 bit), 2 (1024 bit), and 5 (1536 bit) are not allowed. **Note** The key size restrictions disable use of IKEv1 with FIPS. • Restrictions on the Hash Algorithm for Digital Signatures—Only SHA256 or better is allowed. • SSH Cipher Restrictions—Allowed ciphers: aes128-cbc or aes256-cbc. MACs: SHA1 To see the FIPS certification status for the ASA, see: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf This PDF is updated weekly. See the Computer Security Division Computer Security Resource Center site for more information: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html We modified the following command: **fips enable**
Firewall Features	
Improved SIP inspection performance on multiple core ASAs.	If you have multiple SIP signaling flows going through an ASA with multiple cores, SIP inspection performance has been improved. However, you will not see improved performance if you are using a TLS, phone, or IME proxy. We did not modify any commands.
SIP inspection support for Phone Proxy and UC-IME Proxy was removed.	You can no longer use Phone Proxy or UC-IME Proxy when configuring SIP inspection. Use TLS Proxy to inspect encrypted traffic. We removed the following commands: **phone-proxy**, **uc-ime**. We removed the **phone-proxy** and **uc-ime** keywords from the **inspect sip** command.

Feature	Description
DCERPC inspection support for ISystemMapper UUID message RemoteGetClassObject opnum3.	The ASA started supporting non-EPM DCERPC messages in release 8.3, supporting the ISystemMapper UUID message RemoteCreateInstance opnum4. This change extends support to the RemoteGetClassObject opnum3 message. We did not modify any commands.
Unlimited SNMP server trap hosts per context	The ASA supports an unlimited number of SNMP server trap hosts per context. The **show snmp-server host** command output displays only the active hosts that are polling the ASA, as well as the statically configured hosts. We modified the following command: **show snmp-server host**.
VXLAN packet inspection	The ASA can inspect the VXLAN header to enforce compliance with the standard format. We introduced the following command: **inspect vxlan**.
DHCP monitoring for IPv6	You can now monitor DHCP statistics and DHCP bindings for IPv6.
ESMTP inspection change in default behavior for TLS sessions.	The default for ESMTP inspection was changed to allow TLS sessions, which are not inspected. However, this default applies to new or reimaged systems. If you upgrade a system that includes **no allow-tls**, the command is not changed. The change in default behavior was also made in these older versions: 8.4(7.25), 8.5(1.23), 8.6(1.16), 8.7(1.15), 9.0(4.28), 9.1(6.1), 9.2(3.2) 9.3(1.2), 9.3(2.2).
High Availability Features	
Blocking syslog generation on a standby ASA	You can now block specific syslogs from being generated on a standby unit. We introduced the following command: **no logging message** *syslog-id* **standby**.
Enable and disable ASA cluster health monitoring per interface	You can now enable or disable health monitoring per interface. Health monitoring is enabled by default on all port-channel, redundant, and single physical interfaces. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored. You might want to disable health monitoring of non-essential interfaces, for example, the management interface. We introduced the following command: **health-check monitor-interface.**
ASA clustering support for DHCP relay	You can now configure DHCP relay on the ASA cluster. Client DHCP requests are load-balanced to the cluster members using a hash of the client MAC address. DHCP client and server functions are still not supported. We introduced the following command: **debug cluster dhcp-relay**
SIP inspection support in ASA clustering	You can now configure SIP inspection on the ASA cluster. A control flow can be created on any unit (due to load balancing), but its child data flows must reside on the same unit. TLS Proxy configuration is not supported. We introduced the following command: **show cluster service-policy**
Routing Features	

Feature	Description
Policy Based Routing	Policy Based Routing (PBR) is a mechanism by which traffic is routed through specific paths with a specified QoS using ACLs. ACLs let traffic be classified based on the content of the packet’s Layer 3 and Layer 4 headers. This solution lets administrators provide QoS to differentiated traffic, distribute interactive and batch traffic among low-bandwidth, low-cost permanent paths and high-bandwidth, high-cost switched paths, and allows Internet service providers and other organizations to route traffic originating from various sets of users through well-defined Internet connections. We introduced the following commands: **set ip next-hop verify-availability, set ip next-hop, set ip next-hop recursive, set interface, set ip default next-hop, set default interface, set ip df, set ip dscp, policy-route route-map, show policy-route, debug policy-route**
Interface Features	
VXLAN support	VXLAN support was added, including VXLAN tunnel endpoint (VTEP) support. You can define one VTEP source interface per ASA or security context. We introduced the following commands: **debug vxlan, default-mcast-group, encapsulation vxlan, inspect vxlan, interface vni, mcast-group, nve, nve-only, peer ip, segment-id, show arp vtep-mapping, show interface vni, show mac-address-table vtep-mapping, show nve, show vni vlan-mapping, source-interface, vtep-nve, vxlan port**
Monitoring Features	
Memory tracking for the EEM	We have added a new debugging feature to log memory allocations and memory usage, and to respond to memory logging wrap events. We introduced or modified the following commands: **memory logging, show memory logging, show memory logging include, event memory-logging-wrap**
Troubleshooting crashes	The **show tech-support** command output and **show crashinfo** command output includes the most recent 50 lines of generated syslogs. Note that you must enable the **logging buffer** command to enable these results to appear.
Remote Access Features	

Feature	Description
Support for ECDHE-ECDSA ciphers	TLSv1.2 added support for the following ciphers: • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 **Note** ECDSA and DHE ciphers are the highest priority. We introduced the following command: **ssl ecdh-group**.
Clientless SSL VPN session cookie access restriction	You can now prevent a Clientless SSL VPN session cookie from being accessed by a third party through a client-side script such as Javascript. **Note** Use this feature only if Cisco TAC advises you to do so. Enabling this command presents a security risk because the following Clientless SSL VPN features will not work without any warning. • Java plug-ins • Java rewriter • Port forwarding • File browser • Sharepoint features that require desktop applications (for example, MS Office applications) • AnyConnect Web launch • Citrix Receiver, XenDesktop, and Xenon • Other non-browser-based and browser plugin-based applications We introduced the following command: **http-only-cookie**. *This feature is also in 9.2(3).*

Feature	Description
Virtual desktop access control using security group tagging	The ASA now supports security group tagging-based policy control for Clientless SSL remote access to internal applications and websites. This feature uses Citrix's virtual desktop infrastructure (VDI) with XenDesktop as the delivery controller and the ASA's content transformation engine. See the following Citrix product documentation for more information: • Policies for XenDesktop and XenApp: http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • Managing policies in XenDesktop 7: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • Using group policy editor for XenDesktop 7 policies: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html
OWA 2013 feature support has been added for Clientless SSL VPN	Clientless SSL VPN supports the new features in OWA 2013 except for the following: • Support for tablets and smartphones • Offline mode • Active Directory Federation Services (AD FS) 2.0. The ASA and AD FS 2.0 can't negotiate encryption protocols. We did not modify any commands.
Citrix XenDesktop 7.5 and StoreFront 2.5 support has been added for Clientless SSL VPN	Clientless SSL VPN supports the access of XenDesktop 7.5 and StoreFront 2.5. See http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html for the full list of XenDesktop 7.5 features, and for more details. See http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html for the full list of StoreFront 2.5 features, and for more details. We did not modify any commands.
Periodic certificate authentication	When you enable periodic certificate authentication, the ASA stores certificate chains received from VPN clients and re-authenticates them periodically. We introduced or modified the following commands: **periodic-authentication certificate, revocation-check, show vpn-sessiondb**
Certificate expiration alerts	The ASA checks all CA and ID certificates in the trust points for expiration once every 24 hours. If a certificate is nearing expiration, a syslog will be issued as an alert. You can configure the reminder and recurrence intervals. By default, reminders will start at 60 days prior to expiration and recur every 7 days. We introduced or modified the following commands: **crypto ca alerts expiration**

Feature	Description
Enforcement of the basic constraints CA flag	Certificates without the CA flag now cannot be installed on the ASA as CA certificates by default. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. You can configure the ASA to allow installation of these certificates if desired. We introduced the following command: **ca-check**
IKEv2 invalid selectors notification configuration	Currently, if the ASA receives an inbound packet on an SA, and the packet's header fields are not consistent with the selectors for the SA, then the ASA discards the packet. You can now enable or disable sending an IKEv2 notification to the peer. Sending this notification is disabled by default. **Note** This feature is supported with AnyConnect 3.1.06060 and later. We introduced the following command: **crypto ikev2 notify invalid-selectors**
IKEv2 pre-shared key in Hex	You can now configure the IKEv2 pre-shared keys in hex. We introduced the following command: **ikev2 local-authentication pre-shared-key hex**, **ikev2 remote-authentication pre-shared-key hex**
Administrative Features	
ASDM management authorization	You can now configure management authorization separately for HTTP access vs. Telnet and SSH access. We introduced the following command: **aaa authorization http console**
ASDM Username From Certificate Configuration	When you enable ASDM certificate authentication (**http authentication-certificate**), you can configure how ASDM extracts the username from the certificate; you can also enable pre-filling the username at the login prompt. We introduced the following command: **http username-from-certificate**
terminal interactive command to enable or disable help when you enter **?** at the CLI	Normally, when you enter **?** at the ASA CLI, you see command help. To be able to enter **?** as text within a command (for example, to include a ? as part of a URL), you can disable interactive help using the **no terminal interactive** command. We introduced the following command: terminal interactive
REST API Features	
REST API Version 1.1	We added support for the REST API Version 1.1.
Support for token-based authentication (in addition to existing basic authentication)	Client can send log-in request to a specific URL; if successful, a token is returned (in response header). Client then uses this token (in a special request header) for sending additional API calls. The token is valid until explicitly invalidated, or the idle/session timeout is reached.

Feature	Description
Limited multiple-context support	The REST API agent can now be enabled in multi-context mode; the CLI commands can be issued only in system-context mode (same commands as single-context mode). Pass-through CLI API commands can be used to configure any context, as follows. `https://<asa_admin_context_ip>/api/cli?context=<context_name>` If the **context** parameter is not present, it is assumed that the request is directed to the **admin** context.
Advanced (granular) inspection	Granular inspection of these protocols is supported: • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP Options • NetBIOS Name Server over IP • SQL*Net

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.

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