



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.



Note ASDM supports many ASA versions. The ASDM documentation and online help includes all of the latest features supported by the ASA. If you are running an older version of ASA software, the documentation might include features that are not supported in your version. Please refer to the feature history table for each chapter to determine when features were added. For the minimum supported version of ASDM for each ASA version, see Cisco ASA Compatibility. See also [Special, Deprecated, and Legacy Services, on page 15](#).

- [ASDM Requirements, on page 1](#)
- [Hardware and Software Compatibility, on page 4](#)
- [VPN Compatibility, on page 5](#)
- [New Features, on page 5](#)
- [Firewall Functional Overview, on page 11](#)
- [VPN Functional Overview, on page 14](#)
- [Security Context Overview, on page 15](#)
- [ASA Clustering Overview, on page 15](#)
- [Special, Deprecated, and Legacy Services, on page 15](#)

ASDM Requirements

ASDM Java Requirements

You can install ASDM using Oracle JRE 8.0. OpenJRE is not supported.



Note ASDM is not tested on Linux.

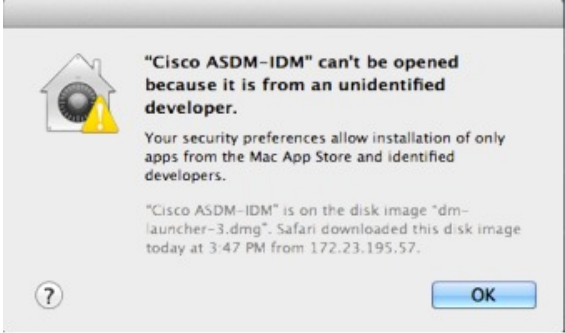
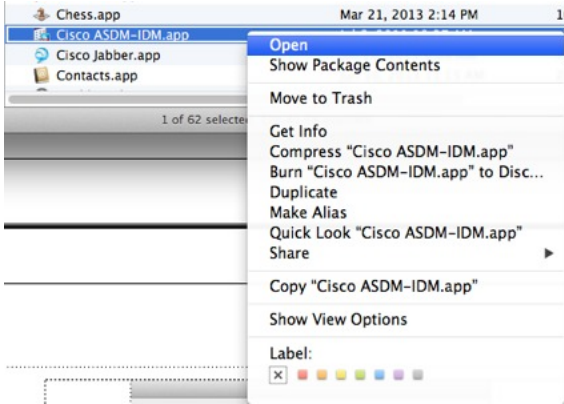

Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

Operating System	Browser				Oracle JRE
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): 10 8 7 Server 2012 R2 Server 2012 Server 2008	Yes	Yes	No support	Yes	8.0
Apple OS X 10.4 and later	No support	Yes	Yes	Yes (64-bit version only)	8.0

ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
Windows 10	<p>"This app can't run on your PC" error message.</p> <p>When you install the ASDM Launcher, Windows 10 might replace the ASDM shortcut target with the Windows Scripting Host path, which causes this error. To fix the shortcut target:</p> <ol style="list-style-type: none"> 1. Choose Start > Cisco ASDM-IDM Launcher, and right-click the Cisco ASDM-IDM Launcher application. 2. Choose More > Open file location. Windows opens the directory with the shortcut icon. 3. Right click the shortcut icon, and choose Properties. 4. Change the Target to: C:\Windows\System32\wscript.exe invisible.vbs run.bat 5. Click OK.
OS X	<p>On OS X, you may be prompted to install Java the first time you run ASDM; follow the prompts as necessary. ASDM will launch after the installation completes.</p>

Conditions	Notes
OS X 10.8 and later	<p>You need to allow ASDM to run because it is not signed with an Apple Developer ID. If you do not change your security preferences, you see an error screen.</p>  <p>371051</p> <ol style="list-style-type: none"> To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose Open.  <p>371052</p> <ol style="list-style-type: none"> You see a similar error screen; however, you can open ASDM from this screen. Click Open. The ASDM-IDM Launcher opens.  <p>371053</p>

Conditions	Notes
<p>Requires Strong Encryption license (3DES/AES) on ASA</p> <p>Note Smart licensing models allow initial access with ASDM without the Strong Encryption license.</p>	<p>ASDM requires an SSL connection to the ASA. You can request a 3DES license from Cisco:</p> <ol style="list-style-type: none"> 1. Go to www.cisco.com/go/license. 2. Click Continue to Product License Registration. 3. In the Licensing Portal, click Get Other Licenses next to the text field. 4. Choose IPS, Crypto, Other... from the drop-down list. 5. Type ASA in to the Search by Keyword field. 6. Select Cisco ASA 3DES/AES License in the Product list, and click Next. 7. Enter the serial number of the ASA, and follow the prompts to request a 3DES/AES license for the ASA.
<ul style="list-style-type: none"> • Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari 	<p>When the ASA uses a self-signed certificate or an untrusted certificate, Firefox and Safari are unable to add security exceptions when browsing using HTTPS over IPv6. See https://bugzilla.mozilla.org/show_bug.cgi?id=633001. This caveat affects all SSL connections originating from Firefox or Safari to the ASA (including ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority.</p>
<ul style="list-style-type: none"> • SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome. • Chrome 	<p>If you change the SSL encryption on the ASA to exclude both RC4-MD5 and RC4-SHA1 algorithms (these algorithms are enabled by default), then Chrome cannot launch ASDM due to the Chrome “SSL false start” feature. We suggest re-enabling one of these algorithms (see the Configuration > Device Management > Advanced > SSL Settings pane); or you can disable SSL false start in Chrome using the --disable-ssl-false-start flag according to Run Chromium with flags.</p>
<p>IE9 for servers</p>	<p>For Internet Explorer 9.0 for servers, the “Do not save encrypted pages to disk” option is enabled by default (See Tools > Internet Options > Advanced). This option causes the initial ASDM download to fail. Be sure to disable this option to allow ASDM to download.</p>

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 ASDM 7.9(2.152)

Released: May 9, 2018

Feature	Description
VPN Features	
Support for legacy SAML authentication	<p>If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6. This option will be deprecated in the near future.</p> <p>New/Modified screens:</p> <p>Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles page > Connection Profiles area > Add button > Add AnyConnect Connection Profile dialog box</p> <p>Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > page > Connection Profiles area > Add button > Add Clientless SSL VPN Connection Profile dialog box</p> <p>New/Modified options: SAML External Browser check box</p>

New Features in ASA 9.9(2)/ASDM 7.9(2)

Released: March 26, 2018

Feature	Description
Platform Features	

Feature	Description
ASAv support for VMware ESXi 6.5	The ASAv virtual platform supports hosts running on VMware ESXi 6.5. New VMware hardware versions have been added to the <i>vi.ovf</i> and <i>esxi.ovf</i> files to enable optimal performance and usability of the ASAv on ESXi 6.5. We did not modify any screens.
ASAv support for VMXNET3 interfaces	The ASAv virtual platform supports VMXNET3 interfaces on VMware hypervisors. We did not modify any screens.
ASAv support for virtual serial console on first boot	You can now configure the ASAv to use the virtual serial console on first boot, instead of the virtual VGA console, to access and configure the ASAv.
ASAv support to update user-defined routes in more than one Azure subscription for High Availability on Microsoft Azure	You can now configure the ASAv in an Azure High Availability configuration to update user-defined routes in more than one Azure subscription. New or modified screens: Configuration > Device Management > High Availability and Scalability > Failover > Route-Table
VPN Features	
Remote Access VPN multi-context support extended to IKEv2 protocol	Support for configuring ASA to allow Anyconnect and third party Standards-based IPsec IKEv2 VPN clients to establish Remote Access VPN sessions to ASA operating in multi-context mode.
IPv6 connectivity to Radius Servers	ASA 9.9.2 now supports IPv6 connectivity to external AAA Radius Servers.
Easy VPN Enhancements for BVI Support	Easy VPN has been enhanced to support a Bridged Virtual Interface (BVI) as its internal secure interface, and you can now directly configure which interface to use as the internal secure interface. Otherwise, the ASA chooses its internal secure interface using security levels. Also, management services, such as telnet , http , and ssh , can now be configured on a BVI if VPN management-access has been enabled on that BVI. For non-VPN management access, you should continue to configure these services on the bridge group member interfaces.
Distributed VPN Session Improvements	<ul style="list-style-type: none"> • The Active Session Redistribution logic, which balances Distributed S2S VPN active and backup sessions, has been improved. Also, the balancing process may be repeated up to eight times in the background for a single cluster redistribute vpn-sessiondb command entered by the administrator. • The handling of dynamic Reverse Route Injections (RRI) across the cluster has been improved.
High Availability and Scalability Features	
Automatically rejoin the cluster after an internal failure	Formerly, many error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals by default: 5 minutes, 10 minutes, and then 20 minutes. These values are configurable. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New or modified screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster > Auto Rejoin

Feature	Description
Configurable debounce time to mark an interface as failed for the ASA 5000-X series	<p>You can now configure the debounce time before the ASA considers an interface to be failed and the unit is removed from the cluster on the ASA 5500-X series. This feature allows for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the ASA waits the number of milliseconds specified before marking the interface as failed and the unit is removed from the cluster. The default debounce time is 500 ms, with a range of 300 ms to 9 seconds. This feature was previously available for the Firepower 4100/9300.</p> <p>New or modified screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster</p>
Show transport related statistics for cluster reliable transport protocol messages	<p>You can now view per-unit cluster reliable transport buffer usage so you can identify packet drop issues when the buffer is full in the control plane.</p> <p>New or modified command: show cluster info transport cp detail</p>
Show failover history from peer unit	<p>You can now view failover history from the peer unit, using the details keyword . This includes failover state changes and reason for the state change.</p> <p>New or modified command: show failover</p>
Interface Features	
Unique MAC address generation for single context mode	<p>You can now enable unique MAC address generation for VLAN subinterfaces in single context mode. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses.</p> <p>New or modified command: mac-address auto</p> <p>No ASDM support.</p> <p><i>Also in 9.8(3) and 9.8(4).</i></p>
Administrative Features	
RSA key pair supports 3072-bit keys	<p>You can now set the modulus size to 3072.</p> <p>New or modified screen: Configuration > Device Management > Certificate Management > Identity Certificates</p>
The FXOS bootstrap configuration now sets the enable password	<p>When you deploy the ASA on the Firepower 4100/9300, the password setting in the bootstrap configuration now sets the enable password as well as the admin user password. Requires FXOS Version 2.3.1.</p>
Monitoring and Troubleshooting Features	

Feature	Description
SNMP IPv6 support	<p>The ASA now supports SNMP over IPv6, including communicating with SNMP servers over IPv6, allowing the execution of queries and traps over IPv6, and supporting IPv6 addresses for existing MIBs. We added the following new SNMP IPv6 MIB objects as described in RFC 8096.</p> <ul style="list-style-type: none"> • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30)—Contains per-interface IPv6-specific information. • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32)—Includes all the prefixes learned by this entity. • ipAddressTable (OID: 1.3.6.1.2.1.4.34)—Contains addressing information relevant to the entity's interfaces. • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35)—Contains the mapping from IP addresses to physical addresses. <p>New or modified screen: Configuration > Device Management > Management Access > SNMP</p>
Conditional Debugging to troubleshoot a single user session	<p>Conditional debugging feature now assists you to verify the logs of specific ASA VPN sessions based on the filter conditions that are set. Support for "any, any" for IPv4 and IPv6 subnets is provided.</p>

New Features in ASDM 7.9(1.151)

Released: February 14, 2018

There are no new features in this release.

New Features in ASA 9.9(1)/ASDM 7.9(1)

Released: December 4, 2017

Feature	Description
Firewall Features	
Ethertype access control list changes	<p>EtherType access control lists now support Ethernet II IPX (EII IPX). In addition, new keywords are added to the DSAP keyword to support common DSAP values: BPDU (0x42), IPX (0xE0), Raw IPX (0xFF), and ISIS (0xFE). Consequently, existing EtherType access control entries that use the BPDU or ISIS keywords will be converted automatically to use the DSAP specification, and rules for IPX will be converted to 3 rules (DSAP IPX, DSAP Raw IPX, and EII IPX). In addition, packet capture that uses IPX as an EtherType value has been deprecated, because IPX corresponds to 3 separate EtherTypes.</p> <p>New or modified screen: Configuration > Firewall > EtherType Rules.</p>
VPN Features	

Feature	Description
Distributed Site-to-Site VPN with clustering on the Firepower 9300	<p>An ASA cluster on the Firepower 9300 supports Site-to-Site VPN in distributed mode. Distributed mode provides the ability to have many Site-to-Site IPsec IKEv2 VPN connections distributed across members of an ASA cluster, not just on the control unit (as in centralized mode). This significantly scales VPN support beyond Centralized VPN capabilities and provides high availability. Distributed S2S VPN runs on a cluster of up to two chassis, each containing up to three modules (six total cluster members), each module supporting up to 6K active sessions (12K total), for a maximum of approximately 36K active sessions (72K total).</p> <p>New or modified screens:</p> <p>Monitoring > ASA Cluster > ASA Cluster > VPN Cluster Summary</p> <p>Monitoring > VPN > VPN Statistics > Sessions</p> <p>Configuration > Device Management > High Availability and Scalability > ASA Cluster Wizards > Site-to-Site</p> <p>Monitoring > VPN > VPN Statistics > Sessions</p> <p>Monitoring > ASA Cluster > ASA Cluster > VPN Cluster Summary</p> <p>Monitoring > ASA Cluster > ASA Cluster > System Resource Graphs > CPU/Memory</p> <p>Monitoring > Logging > Real-Time Log Viewer</p>
High Availability and Scalability Features	
Active/Backup High Availability for ASAv on Microsoft Azure	<p>A stateless Active/Backup solution that allows for a failure of the active ASAv to trigger an automatic failover of the system to the backup ASAv in the Microsoft Azure public cloud.</p> <p>New or modified screens: Configuration > Device Management > High Availability and Scalability > Failover</p> <p>Monitoring > Properties > Failover > Status</p> <p>Monitoring > Properties > Failover > History</p> <p><i>Also in 9.8(1.200).</i></p>
Improved chassis health check failure detection for the Firepower chassis	<p>You can now configure a lower holdtime for the chassis health check: 100 ms. The previous minimum was 300 ms.</p> <p>New or modified command: app-agent heartbeat interval</p> <p>No ASDM support.</p>
Inter-site redundancy for clustering	<p>Inter-site redundancy ensures that a backup owner for a traffic flow will always be at the other site from the owner. This feature guards against site failure.</p> <p>New or modified screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster</p>

Feature	Description
cluster remove unit command behavior matches no enable behavior	<p>The cluster remove unit command now removes a unit from the cluster until you manually reenables clustering or reload, similar to the no enable command. Previously, if you redeployed the bootstrap configuration from FXOS, clustering would be reenabled. Now, the disabled status persists even in the case of a bootstrap configuration redeployment. Reloading the ASA, however, will reenables clustering.</p> <p>New/Modified screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster</p>
Administrative, Monitoring, and Troubleshooting Features	
SSH version 1 has been deprecated	<p>SSH version 1 has been deprecated, and will be removed in a future release. The default setting has changed from both SSH v1 and v2 to just SSH v2.</p> <p>New/Modified screens:</p> <ul style="list-style-type: none"> • Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
Enhanced packet tracer and packet capture capabilities	<p>The packet tracer has been enhanced with the following features:</p> <ul style="list-style-type: none"> • Trace a packet when it passes between cluster units. • Allow simulated packets to egress the ASA. • Bypass security checks for a simulated packet. • Treat a simulated packet as an IPsec/SSL decrypted packet. <p>The packet capture has been enhanced with the following features:</p> <ul style="list-style-type: none"> • Capture packets after they are decrypted. • Capture traces and retain them in the persistent list. <p>New or modified screens:</p> <p>Tools > Packet Tracer</p> <p>We added Cluster Capture field to support these options: decrypted, persist, bypass-checks, transmit</p> <p>We added two new options in the Filter By view under the All Sessions drop-down list: Origin and Origin-ID</p> <p>Monitoring > VPN > VPN Statistics > Packet Tracer and Capture</p> <p>We added ICMP Capture field in the Packet Capture Wizard screen: Wizards > Packet Capture Wizard</p> <p>We added two options include-decrypted and persist to support ICMP Capture.</p>

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, Deprecated, 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](#)

Deprecated Services

For deprecated features, see the configuration guide for your ASA version. Similarly, for redesigned features such as NAT between Version 8.2 and 8.3 or transparent mode interfaces between Version 8.3 and 8.4, refer to the configuration guide for your version. Although ASDM is backwards compatible with previous ASA releases, the configuration guide and online help only cover the latest release.

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