

Introduction to the Secure Firewall ASA

The Secure Firewall ASA provides advanced stateful firewall and VPN concentrator functionality in one device. 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 18.

- ASDM Requirements, on page 1
- Hardware and Software Compatibility, on page 7
- VPN Compatibility, on page 7
- New Features, on page 7
- Firewall Functional Overview, on page 14
- VPN Functional Overview, on page 17
- Security Context Overview, on page 18
- ASA Clustering Overview, on page 18
- Special, Deprecated, and Legacy Services, on page 18

ASDM Requirements

ASDM Java Requirements

You can install ASDM using Oracle JRE 8.0 (**asdm-*version*.bin**) or OpenJRE 1.8.x (**asdm-openjre-*version*.bin**).

The Oracle version of ASDM is included in the ASA package; if you want to use the OpenJRE version, you will need to copy it to the ASA and configure the ASA to use that version of ASDM.

Note ASDM is not supported on Linux.

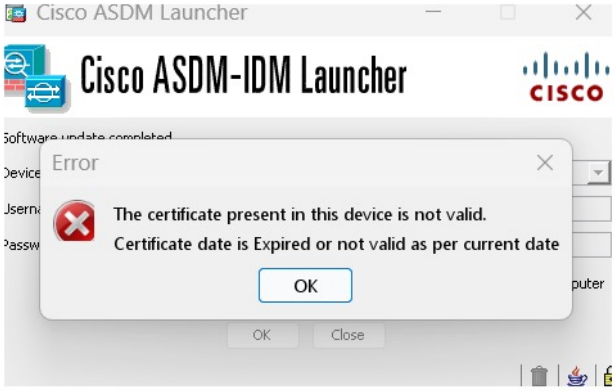
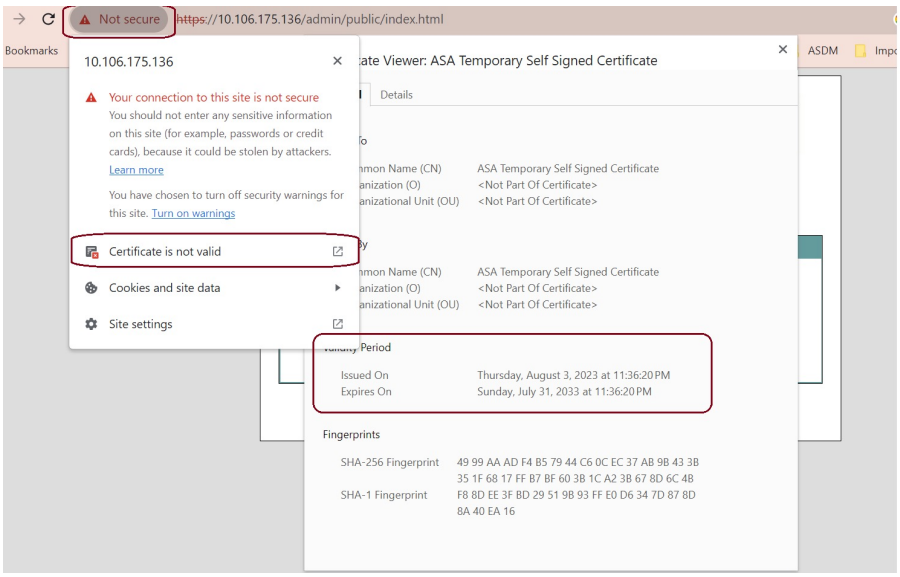
Table 1: ASDM Operating System and Browser Requirements

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): • 11 • 10 **Note** See Windows 10 in ASDM Compatibility Notes, on page 2 if you have problems with the ASDM shortcut. • 8 • 7 • Server 2016 and Server 2019 • Server 2012 R2 • Server 2012 • Server 2008	Yes	No support	Yes	8.0 version 8u261 or later	1.8 **Note** No support for Windows 7 or 10 32-bit
Apple OS X 10.4 and later	Yes	Yes	Yes (64-bit version only)	8.0 version 8u261 or later	1.8

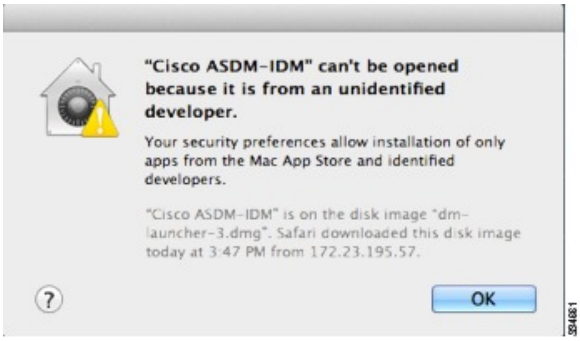
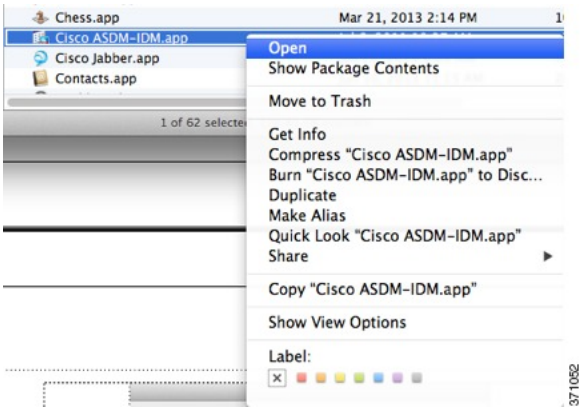
ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
ASDM Launcher compatibility with ASDM version	"**Unable to Launch Device Manager**" error message. If you upgrade to a new ASDM version and then get this error, you may need to re-install the latest Launcher. **1.** Open the ASDM web page on the ASA: https://<asa_ip_address>. **2.** Click **Install ASDM Launcher**. ***Figure 1: Install ASDM Launcher***  **3.** Leave the username and password fields empty (for a new installation), and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. When you enter the **enable** command at the CLI for the first time, you are prompted to change the password; this behavior is not enforced when you log into ASDM. We suggest that you change the enable password as soon as possible so that it does not remain blank. **Note**: If you enabled HTTPS authentication, enter your username and associated password. Even without authentication, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

Conditions	Notes
Self-signed certificate not valid due to a time and date mismatch with ASA	ASDM validates the self-signed SSL certificate, and if the ASA's date is not within the certificate's **Issued On** and **Expires On** date, ASDM will not launch. If there is a time and date mismatch, you will see the following error: ***Figure 2: Certificate Not Valid***  **To fix the issue:** Set the correct time on the ASA and reload. To check the certificate dates, (example shown is Chrome): **1.** Go to https://*device_ip*. **2.** Click the **Not secure** text in the menu bar. **3.** Click **Certificate is not valid** to open the Certificate Viewer. **4.** Check the Validity Period. ***Figure 3: Certificate Viewer*** 

Conditions	Notes
Windows Active Directory directory access	In some cases, Active Directory settings for Windows users may restrict access to program file locations needed to successfully launch ASDM on Windows. Access is needed to the following directories: • Desktop folder • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems If your Active Directory is restricting directory access, you need to request access from your Active Directory administrator.
Windows 10	"**This app can't run on your PC**" error message. 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: **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	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.

Conditions	Notes
OS X 10.8 and later	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.  **1.** To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose **Open**.  **2.** You see a similar error screen; however, you can open ASDM from this screen. Click **Open**. The ASDM-IDM Launcher opens. 

Conditions	Notes
(ASA 5500 and ISA 3000) Requires Strong Encryption license (3DES/AES) on ASA **Note** Smart licensing models allow access with ASDM without the Strong Encryption license.	ASDM requires an SSL connection to the ASA. You can request a 3DES PAK license from Cisco: 1. Go to https://www.cisco.com/go/license. 2. Under **Traditional Licenses**, click **Access LRP**. 3. Click **Get Licenses** and then choose **IPS, Crypto, Other...** from the drop-down list. 4. Type **ASA** in to the **Search by Keyword** field. 5. Select **Cisco ASA 3DES/AES License** in the **Product** list, and click **Next**. 6. Enter the serial number of the ASA, and follow the prompts to request a 3DES/AES license for the ASA.
• Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari	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.
• SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome. • Chrome	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.

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 9.20(4)/ASDM 7.20(4)

Released: July 2, 2025

Feature	Description
License Features	
Smart Transport is the default Smart Licensing transport	Smart Licensing now uses Smart Transport as the default transport. You can optionally enable the former type, Smart Call Home, if necessary. New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing** *Also in 9.22(1).*
Administrative, Monitoring, and Troubleshooting Features	
SSH X.509 certificate authentication	You can now use an X.509v3 certificate to authenticate a user for SSH (RFC 6187). For the Firepower 4100/9300, you need FXOS version 2.16(2.109+) or 2.18+. **Note** The bundled version of ASDM 7.20(4) does not include support for this feature. Download and install ASDM 7.20(4) from Cisco.com for feature support. Be sure to change the image name to asdm.bin if you want to overwrite the bundled version. New/Modified screens: • **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authorization** • **Configuration** > **Device Management** > **Certificate Management** > **CA Certificates** > **Add/Edit Trustpoint** > **Advanced** • **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** *Also in 9.22(3), 9.24(1).*
AES-256-GCM SSH cipher	The ASA supports the AES-256-GCM cipher for SSH. It is enabled by default for **all** and **high** encryption levels. New/Modified screens: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** *Also in 9.22(3), 9.24(1).*
Display of UDP's initiator and responder values in connection status output	For UDP traffic flows, the ASA displays the initiator and responder field values in the connection detail status. These field values indicate the direction of communication, which helps in troubleshooting network connectivity issues.

New Features in ASA 9.20(3)

Released: July 31, 2024

Feature	Description
Platform Features	
ASA Virtual AWS IMDSv2 support	AWS Instance Metadata Service version 2 (IMDSv2) API is now supported on ASA Virtual, which allows you to retrieve and validate instance metadata. IMDSv2 provides additional security against vulnerabilities targeting the Instance Metadata Service. When deploying ASA Virtual on AWS, you can now configure the Metadata version for ASA Virtual as follows: • ASA Virtual 9.20(3) and later supports IMDSv2 only (token required) – Set "V2 only (token required)" to enable IMDSv2. • Earlier ASA Virtual versions support only IMDSv1 APIs via the IMDS option - 'IMDSv1 or IMDSv2 (token optional)' – Set "V1 and V2 (token optional). If you have an existing ASA Virtual deployment, you can migrate to "IMDSv2 Required" mode after upgrading to 9.20(3) and later. See AWS documentation, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-options.html For more information, see Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.20.
Firewall Features	
Threat Detection for VPN services	You can configure threat detection for VPN services to protect against the following types of VPN attack from IPv4 addresses: • Excessive failed authentication attempts to a remote access VPN, for example brute-force username/password scanning. • Client initiation attacks, where the attacker starts but does not complete repeated connection attempts to a remote access VPN head-end from a single host. • Access attempts to invalid VPN services, that is, services that are for internal use only. These attacks, even when unsuccessful in their attempt to gain access, can consume computational resources and in some cases result in Denial of Service. The following commands were introduced or changed: **clear threat-detection service**, **show threat-detection service**, **shun**, **threat-detection service**.
VPN Features	
Multiple IdP certificates in a webvpn configuration and a tunnel-group	You can now configure tunnel-group-specific IdP certificates and multiple IdP certificates in a webvpn configuration. This feature lets you trust an old certificate as well as a new certificate, making migration to the new certificate easier. New/Modified commands: **saml idp-trustpoint**, **trustpoint idp** No ASDM support

Feature	Description
Rate Limit for Preauthenticated SSL Connections	ASA Virtual can rate-limit preauthenticated SSL connections. This limit is calculated as three times the VPN connection limit of the device. When this limit exceeds, no new SSL connections are allowed. The device allows new SSL connections only after the preauthenticated SSL connections count becomes zero. However, this restriction is not valid for management connections. New/Modified commands: **show counters** No ASDM support

New Features in ASA 9.20(2)/ASDM 7.20(2)

Released: December 13, 2023

Feature	Description
Platform Features	
100GB network module support for the Secure Firewall 3100	You can now use the 100GB network module for the Secure Firewall 3100. This module is also supported for the Secure Firewall 4200.
Increased connection limits for the Secure Firewall 4200	Connection limits have been increased: • 4215: 15M → **40M** • 4225: 30M → **80M** • 4245: 60M → **80M**
ASAv on OCI: Additional instances	ASA Virtual instances on OCI now supports additional shapes to achieve the highest performance and throughput level.
High Availability and Scalability Features	
ASAv on Azure: Clustering with Gateway Load Balancing	We now support the ASA virtual clustering deployment on Azure using the Azure Resource Manager (ARM) template and then configure the ASAv clusters to use the Gateway Load Balancer (GWLB) for load balancing the network traffic. New/Modified screens:
ASAv on AWS: Resiliency for clustering with Gateway Load Balancing	You can configure the Target Failover option in the Target Groups service of AWS, which helps GWLB to forward existing flows to a healthy target in the event of virtual instance failover. In the ASAv clustering, each instance is associated with a Target Group, where the Target Failover option is enabled. It helps GWLB to identify an unhealthy target and redirect or forward the network traffic to a healthy instance identified or registered as a target node in the target group.

Feature	Description
Configurable delay to rejoin cluster after chassis heartbeat failure (Firepower 4100/9300)	By default, if the chassis heartbeat fails and then recovers, the node rejoins the cluster immediately. However, if you configure the **health-check chassis-heartbeat-delay-rejoin** command, it will rejoin according to the settings of the **health-check system auto-rejoin** command. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Auto Rejoin**
show failover statistics includes client statistics	The failover client packet statistics are now enhanced to improve debuggability. The **show failover statistics** command is enhanced to display **np-clients** (data-path clients) and **cp-clients** (control-plane clients) information. Modified commands: **show failover statistics cp-clients**, **show failover statistics np-clients** *Also in 9.18(4).*
show failover statistics events includes new events	The **show failover statistics events** command is now enhanced to identify the local failures notified by the App agent: failover link uptime, supervisor heartbeat failures, and disk full issues. Modified commands: **show failover statistics events** *Also in 9.18(4).*

New Features in ASA 9.20(1)/ASDM 7.20(1)

Released: September 7, 2023

Note This release is only supported on the Secure Firewall 4200.

Feature	Description
Platform Features	
Secure Firewall 4200	We introduced the ASA for the Secure Firewall 4215, 4225, and 4245. The Secure Firewall 4200 supports up to 8 units for Spanned EtherChannel clustering. You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 4200 25 Gbps and higher interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. There are two Management interfaces.
Firewall Features	
ASDM support for the **sysopt connection tcp-max-unprocessed-seg** command	You can set the maximum number of TCP unprocessed segments, from 6 to 24. The default is 6. If you find that SIP phones are not connecting to the call manager, you can try increasing the maximum number of unprocessed TCP segments. New/Modified screens: **Configuration** > **Firewall** > **Advanced** > **TCP Options**.

Feature	Description
ASP rule engine compilation offloaded to the data plane.	By default, ASP rule engine compilation is offloaded to the data plane (instead of the control plane) when any rule-based policy (for example, ACL, NAT, VPN) has more than 100 rule updates. The offload leaves more time for the control plane to perform other tasks. We added or modified the following commands: **asp rule-engine compile-offload**, **show asp rule-engine**.
High Availability and Scalability Features	
Reduced false failovers for ASA high availability	We now introduced an additional heartbeat module in the data plane of the ASA high availability. This heartbeat module helps to avoid false failovers or split-brain scenarios that can happen due to traffic congestion in the control plain or CPU overload. *Also in 9.18(4).*
Configurable cluster keepalive interval for flow status	The flow owner sends keepalives (clu_keepalive messages) and updates (clu_update messages) to the director and backup owner to refresh the flow state. You can now set the keepalive interval. The default is 15 seconds, and you can set the interval between 15 and 55 seconds. You may want to set the interval to be longer to reduce the amount of traffic on the cluster control link. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration**
Routing Features	
EIGRPv6	You can now configure EIGRP for IPv6 and manage them separately. You must explicitly enable IPv6 when configuring EIGRP on each interface. New/Modified screens: **Configuration** > **Device Setup** > **Routing** > **EIGRPv6** , **Setup**, **Filter Rules**,**Interface**,**Passive Interface**, **Redistribution**, **Static Neighbor** tabs.
Path monitoring through HTTP client	PBR can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. HTTP based path-monitoring can be configured on the interface using Network Service Group objects. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Path Monitoring**
Interface Features	
VXLAN VTEP IPv6 support	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the ASA Virtual cluster control link or for Geneve encapsulation. New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **VXLAN** • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VNI Interface**

Feature	Description
Loopback interface support for DNS, HTTP, ICMP, and IPsec Flow Offload	You can now add a loopback interface and use it for: • DNS • HTTP • ICMP • IPsec Flow Offload
License Features	
IPv6 for Cloud services such as Smart Licensing and Smart Call Home	ASA now supports IPv6 for Cloud services such as Smart Licensing and Smart Call Home.
Certificate Features	
IPv6 PKI for OCSP and CRL	ASA now supports both IPv4 and IPv6 OCSP and CRL URLs. When using IPv6 in the URLs, it must be enclosed with square brackets. New/Modified screens: **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add**
Administrative, Monitoring, and Troubleshooting Features	
Rate limiting for SNMP syslogs	If you do not set system-wide rate limiting, you can now configure rate limiting separately for syslogs sent to an SNMP server. New/Modified commands: **logging history rate-limit**
Packet Capture for switches	You can now configure to capture egress and ingress traffic packets for a switch. This option is applicable only for Secure Firewall 4200 model devices. New/Modified screens: **Wizards** > **Packet Capture Wizard** > **Ingress Traffic Selector**and **Wizards** > **Packet Capture Wizard** > **Egress Traffic Selector**
VPN Features	
Crypto debugging enhancements	Following are the enhancements for crypto debugging: • Crypto archive is now available in two formats: text and binary format. • Additional SSL counters. • Stuck encrypt rules can be removed from the ASP table without rebooting the device.
Multiple Key Exchanges for IKEv2	ASA supports multiple key exchanges in IKEv2 to secure the IPsec communication from quantum computer attacks.

Feature	Description
Secure Client connection authentication using SAML	In a DNS load balancing cluster, when SAML authentication is configured on ASAs, you can specify a local base URL that uniquely resolves to the device on which the configuration is applied. New/Modified screens: **Configuration > Remote Access VPN > Network (Client) Access > Secure Client Connection Profiles > Add/Edit > Basic > SAML Identity Provider > Manage > Add/Edit**
ASDM Features	
Windows 11 support	ASDM has been verified to operate on Windows 11.

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. 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.

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