# 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.



## 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(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:<br>• ASA virtual 9.20(3) and later supports IMDSv2 only (token required) – Set "V2 only (token required)" to enable IMDSv2.<br>• Earlier ASA virtual versions support only IMDSv1 APIs via the IMDS option - 'IMDSv1 or IMDSv2 (token optional)' – Set "V1 and V2 (token optional).<br>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<br>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:<br>• Excessive failed authentication attempts to a remote access VPN, for example brute-force username/password scanning.<br>• 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.<br>• Access attempts to invalid VPN services, that is, services that are for internal use only.<br>These attacks, even when unsuccessful in their attempt to gain access, can consume computational resources and in some cases result in Denial of Service.<br>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.<br>New/Modified commands: **saml idp-trustpoint**, **trustpoint idp** |

| 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.<br>New/Modified commands: **show counters** |

# New Features in ASA 9.20(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:<br>• 4215: 15M → **40M**<br>• 4225: 30M → **80M**<br>• 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.<br>New/Modified commands: |
| 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. |
| 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.<br>New/Modified commands: **health-check chassis-heartbeat-delay-rejoin** |

| Feature | Description |
|---|---|
| **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.<br>Modified commands: **show failover statistics cp-clients**, **show failover statistics np-clients**<br>*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.<br>Modified commands: **show failover statistics events**<br>*Also in 9.18(4).* |

# New Features in ASA 9.20(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** | |
| 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.<br>We added or modified the following commands: **asp rule-engine compile-offload**, **show asp rule-engine**. |
| Data plane quick reload | When data plane needs to be restarted, instead of a reboot of the device, you can now reload the data plane process. When data plane quick reload is enabled, it restarts the data plane and other processes.<br>New/Modified commands:**data-plane quick-reload**, **show data-plane quick-reload status**. |

| Feature | Description |
|---|---|
| **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.<br>*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.<br>New/Modified commands: **clu-keepalive-interval** |
| **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.<br>New/Modified commands: Following are the new commands introduced: **ipv6 eigrp**, **ipv6 hello-interval eigrp**, **ipv6 hold-time eigrp**, **ipv6 split-horizon eigrp**, **show ipv6 eigrp interface** , **show ipv6 eigrp traffic**, **show ipv6 eigrp neighbors** , **show ipv6 eigrp interface**, **ipv6 summary-address eigrp**, **show ipv6 eigrp topology**, **show ipv6 eigrp events** , **show ipv6 eigrp timers**, **clear ipv6 eigrp** , and **clear ipv6 router eigrp**<br>Following commands are modified to support IPv6: **default-metric**, **distribute-list prefix-list**, **passive-interface**, **eigrp log-neighbor-warnings**, **eigrp log-neighbor-changes**, **eigrp router-id**, and **eigrp stub** |
| **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.<br>New/Modified commands: **default-mcast-group**, **mcast-group**, **peer ip** |
| Loopback interface support for DNS, HTTP, ICMP, and IPsec Flow Offload | You can now add a loopback interface and use it for:<br>• DNS<br>• HTTP<br>• ICMP<br>• 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** | |

| Feature | Description |
|---|---|
| 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.<br>New/Modified commands:**crypto ca trustpointcrl**, **cdp url**, **ocsp url** |
| **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.<br>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.<br>New/Modified commands:<br>**capture** *capture_name* **switch interface** *interface_name* [ **direction** { **both** \| **egress** \| **ingress** } ] |
| **VPN Features** | |
| Crypto debugging enhancements | Following are the enhancements for crypto debugging:<br>• Crypto archive is now available in two formats: text and binary format.<br>• Additional SSL counters.<br>• Stuck encrypt rules can be removed from the ASP table without rebooting the device.<br>New/Modified commands:<br>• **show counters** |
| Multiple Key Exchanges for IKEv2 | ASA supports multiple key exchanges in IKEv2 to secure the IPsec communication from quantum computer attacks.<br>New/Modified commands: **additional-key-exchange** |

# 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 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