

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, on page 1
- VPN Compatibility, on page 1
- New Features, on page 1
- Firewall Functional Overview, on page 6
- VPN Functional Overview, on page 10
- Security Context Overview, on page 10
- ASA Clustering Overview, on page 11
- Special and Legacy Services, on page 11

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 9.22(3)

Released: March 26, 2026

Feature	Description
Firewall Features	
Changed output for the **show access-list element-count** and **show asp table network-object** commands.	The **show access-list element-count** command now shows 2 counts: total number of objects, and total number of access control entries. The **show asp table network-object** count information includes new counters for the number of additions to the source table and number of those additions to the source table that are duplicate. In addition, the Hitcnt (hit count) column was removed. New/Modified commands: **show access-list element-count**, **show asp table network-object**
High Availability and Scalability Features	
ASAc High Availability and SR-IOV feature enablement	This enables High Availability (HA) support for ASA container (ASAc) deployments in Docker and Kubernetes environments. Two ASAc container instances can be deployed on separate Docker hosts and configured as a primary–secondary failover pair. SR-IOV feature supports single Root I/O virtualization (SR-IOV) interfaces in ASAc container deployments within Docker and Kubernetes environments.
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+. New/Modified commands: **aaa authorization exec ssh-x509**, **ssh authentication method**, **ssh trustpoint sign**, **ssh username-from-certificate**, **validation-usage ssh-client** *Also in 9.20(4), 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 commands: **ssh cipher encryption** *Also in 9.20(4), 9.24(1).*
Message-of-the-day (motd) banner shows the failover state and the last failover time	When using failover, if you configure the **banner motd** command, then the banner shows information about the failover state and the last failover time of the unit you are logging into. This information is useful if you are performing actions at the CLI, such as troubleshooting, and a failover occurs between sessions. New or modified commands: **banner motd** *Also in 9.24(1).*

Feature	Description
Automated Certificate Management Environment (ACME) protocol for TLS device certificates.	You can configure Automated Certificate Management Environment (ACME) protocol to ASA trustpoint to manage the TLS device certificates. ACME enables simplified certificate management through auto renewal, domain validation, and easy enrolling and revoking of certificates. You can choose to use the Let's Encrypt CA server or use any other ACME server for the authentication. ACME uses http01 method for authentication. New or modified commands: **crypto ca trustpoint enrollment protocol crypto ca authenticate** *Also in 9.23(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/Modified commands: **show conn detail** *Also in 9.20(4), 9.24(1).*
Block depletion monitoring in failover and standalone units	When block depletion occurs, the ASA collects troubleshooting logs and sends out a syslog. For failover, the ASA fails over to the standby unit. The ASA can also force a crash and reload to recover from depletion. Added/modified commands: **fault-monitor**, **block-depletion**. *Also in 9.23(1).*

New Features in ASA 9.22(2)

Released: April 10, 2025

There are no new features in this release.

New Features in ASA 9.22(1.1)

Released: September 16, 2024

Note 9.22(1) was not released.

Feature	Description
Platform Features	

Feature	Description
Secure Firewall 1210/1220	The Secure Firewall 1210/1220 is a compact desktop firewall with a built-in switch and, depending on the model, Power over Ethernet+ (PoE+). • Secure Firewall 1210CE—Includes 8 1Gbps RJ-45 copper data ports. • Secure Firewall 1210CP—Includes PoE+ on four of those ports. • Secure Firewall 1220CX—Includes two additional 10Gbps SFP+ ports and higher performance.
ASA Virtual Supports Dual-Arm Deployment Mode on AWS with GWLB	ASA Virtual now supports the dual-arm deployment mode on AWS with GWLB. This mode enables ASA Virtual to directly forward internet-bound traffic to the internet through the internet gateway after traffic inspection, while also performing network address translation (NAT). The dual-arm mode differs from the single-arm mode, which helps in routing inspected outbound traffic back to the GWLB, and then to the internet through the internet gateway. The dual-arm mode supports forwarding of inspected traffic from ASA Virtual to the internet in both single VPC and multiple VPC network environments. The advantages of the dual-arm mode in ASA Virtual are: • Minimize traffic hops, thereby reducing traffic latency and improving throughput performance. • Consolidate and inspect outbound traffic from multiple VPCs before forwarding it to the internet. • Provide a cost-effective solution because of reduced infrastructure requirements. For more information, see Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.22.
Deploy the Cisco Secure Firewall ASA container (ASAc) in a Kubernetes or Docker Environment	A container is a software package that bundles up code and associated requirements such as system libraries, system tools, default settings, and so on, to ensure that the application runs successfully in a computing environment. You can deploy the ASA container (ASAc) in an open-source Kubernetes or Docker environment.
ASA Virtual on VMware ESXi support	ASA Virtual on VMware now supports ESXi version 8.0. For more information, see Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.22.
Firewall Features	
Object group search optimization.	The object group search feature has been enhanced to reduce object lookup time when evaluating access control rules to match connections and to reduce CPU overhead. There are no changes to configuring object group search, the optimized behavior happens automatically. We added the following commands in the device CLI, or enhanced command output: **clear asp table network-object**, **debug ac logs**, **packet-tracer**, **show access-list**, **show asp table network-group**, **show object-group**.
High Availability and Scalability Features	

Feature	Description
Secure Firewall 3100 and 4200 maximum cluster nodes increased to 16.	For the Secure Firewall 3100 and 4200, the maximum nodes were increased from 8 to 16.
Secure Firewall 3100 and 4200 cluster Individual interface mode	Individual interfaces are normal routed interfaces, each with their own *Local IP address* used for routing. The *Main cluster IP address* for each interface is a fixed address that always belongs to the control node. When the control node changes, the Main cluster IP address moves to the new control node, so management of the cluster continues seamlessly. Load balancing must be configured separately on the upstream switch. New/Modified commands: **cluster interface-mode individual**
ASA Virtual Clustering deployment support on the AWS Multi-Availability Zone	You can now deploy and configure the ASA virtual cluster across multiple availability zones in an AWS region. The cluster also has dynamic scaling capability (Autoscale), which helps in scaling up or scaling down virtual devices based on demand. Extending the ASA virtual cluster across multiple availability zones in an AWS region enables continuous traffic inspection and dynamic scaling during disaster recovery. For more information, see Deploy a Cluster for the ASA Virtual in a Public Cloud.
MTU ping test from data node on node join	When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size twice the cluster control link MTU. Previously, only the control node sent a ping. If the ping fails, a notification is generated so you can fix the MTU mismatch on connecting switches and try again. Added/modified commands: **show cluster history**.
Interface Features	
For models with built-in-switches, subinterfaces can't use VLAN 1	For models with built-in switches, you cannot create a subinterface using VLAN 1. VLAN 1 is reserved for the logical VLAN interface for switch ports. If you upgrade a 1010 to 9.22(1) or later, and you have assigned VLAN 1 to a subinterface, you must first change the VLAN ID for your subinterface to a new VLAN. After upgrading, VLAN 1 will be removed from the subinterface.
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 commands: **transport proxy**, **transport type**, **transport url**
ASAvU (Unlimited) license to deploy ASA virtuals with 32 cores and 64 cores	ASAvU license achieves maximum throughput on deployments with 32 cores and 64 cores and is supported only on VMware and KVM. New/Modified commands: **throughput level unlimited**
Administrative, Monitoring, and Troubleshooting Features	

Feature	Description
Disable the USB port (disk1)	By default, the type-A USB port (disk1) is enabled and could not be disabled. You can now disable USB port access for security purposes on the following models: • Firepower 1000 • Secure Firewall 3100 • Secure Firewall 4200 This setting is stored in firmware and requires a reload. Moreover, if the USB port is disabled and you downgrade to a version that does not support this feature, the port will remain disabled and you cannot re-enable it without erasing the NVRAM. **Note** This feature does not affect the type-B USB console port, if present. New/Modified commands: **usb-port disable**, **show usb-port**
Block depletion monitoring in failover and standalone units	When block depletion occurs, the ASA collects troubleshooting logs and sends out a syslog. For failover, the ASA fails over to the standby unit. The ASA can also force a crash and reload to recover from depletion. Added/modified commands: **fault-monitor**, **block-depletion**.
VPN Features	
DTLS Crypto Acceleration	Cisco Secure Firewall 4200 and 3100 series support DTLS cryptographic acceleration. The hardware performs DTLS encryption and decryption, and improves the throughput of the DTLS-encrypted and DTLS-decrypted traffic. The hardware also performs optimization of the egress-encrypted packets to improve latency. New/Modified commands: **flow-offload-dtls**, **flow-offload-dtls egress-optimization**

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