



CHAPTER 1

Introduction to the Security Appliance

The adaptive security appliance combines advanced stateful firewall and VPN concentrator functionality in one device. The adaptive security appliance includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPSec and clientless SSL VPN support, and many more features..

This chapter includes the following sections:

- [New Features, page 1-1](#)
- [Firewall Functional Overview, page 1-5](#)
- [VPN Functional Overview, page 1-9](#)
- [Security Context Overview, page 1-10](#)

New Features

This section lists the features added for each maintenance release, and includes the following topics:

- [New Features in Version 8.1\(2\), page 1-1](#)
- [New Features in Version 8.1\(1\), page 1-4](#)

New Features in Version 8.1(2)

[Table 1-1](#) lists the new features for Version 8.1(2).



Note

Version 8.1(x) is only supported on the Cisco ASA 5580 adaptive security appliance.

Table 1-1 New Features for ASA Version 8.1(2)

Feature	Description
Remote Access Features	
Auto Sign-On with Smart Tunnels for IE	<p>This feature lets you enable the replacement of logon credentials for WININET connections. Most Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does not, so it is not supported by this feature. It also supports HTTP-based authentication, therefore form-based authentication does not work with this feature.</p> <p>Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. Also, because of the association with destinations hosts, providing support for an auto sign-on enabled host may not be desirable if you want to deny access to some of the services on that host.</p> <p>To configure a group auto sign-on for smart tunnels, you create a global list of auto sign-on sites, then assign the list to group policies or user names. This feature is not supported with Dynamic Access Policy.</p> <p>In ASDM, see Configuration > Firewall > Advanced > ACL Manager.</p>
Entrust Certificate Provisioning	<p>ASDM 6.1.3 (which lets you manage security appliances running Versions 8.0x and 8.1x) includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA.</p> <p>In ASDM, see Configuration > Remote Access VPN > Certificate Management > Identity Certificates > Enroll ASA SSL VPN head-end with Entrust.</p>
Extended Time for User Reauthentication on IKE Rekey	<p>You can configure the security appliance to give remote users more time to enter their credentials on a Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunnels and a phase 1 rekey occurred, the security appliance prompted the user to authenticate and only gave the user approximately 2 minutes to enter their credentials. If the user did not enter their credentials in that 2 minute window, the tunnel would be terminated. With this new feature enabled, users now have more time to enter credentials before the tunnel drops. The total amount of time is the difference between the new Phase 1 SA being established, when the rekey actually takes place, and the old Phase 1 SA expiring. With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the rekey interval.</p> <p>In ASDM, see Configuration > Device Management > Certificate Management > Identity Certificates.</p>
Persistent IPsec Tunneled Flows	<p>With the persistent IPsec tunneled flows feature enabled, the security appliance preserves and resumes stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dropped when the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP flows allows some older or sensitive applications to keep working through a short-lived tunnel drop. This feature supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a hardware client. It does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the sysopt connection preserve-vpn-flows command. This option is disabled by default.</p> <p>In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options. Check the Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM) checkbox to enable persistent IPsec tunneled flows.</p>
Show Active Directory Groups	<p>The CLI command show ad-groups was added to list the active directory groups. ASDM Dynamic Access Policy uses this command to present the administrator with a list of MS AD groups that can be used to define the VPN policy.</p> <p>In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit DAP > Add/Edit AAA Attribute.</p>

Table 1-1 New Features for ASA Version 8.1(2) (continued)

Feature	Description
Smart Tunnel over Mac OS	Smart tunnels now support Mac OS. In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels.
Firewall Features	
NetFlow Filtering	You can filter NetFlow events based on traffic and event-type, and then send records to different collectors. For example, you can log all flow-create events to one collector, but log flow-denied events to a different collector. See the flow-export event-type command. In ASDM, see Configuration > Firewall > Security Policy > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > NetFlow.
NetFlow Delay Flow Creation Event	For short-lived flows, NetFlow collecting devices benefit from processing a single event as opposed to seeing two events: flow creation and teardown. You can now configure a delay before sending the flow creation event. If the flow is torn down before the timer expires, only the flow teardown event will be sent. See the flow-export delay flow-create command. Note The teardown event includes all information regarding the flow; there is no loss of information. In ASDM, see Configuration > Device Management > Logging > NetFlow.
QoS Traffic Shaping	If you have a device that transmits packets at a high speed, such as the adaptive security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the shape command. See also the crypto ipsec security-association replay command, which lets you configure the IPSec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPSec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms. In ASDM, see Configuration > Firewall > Security Policy > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.

Table 1-1 New Features for ASA Version 8.1(2) (continued)

Feature	Description
TCP Normalization Enhancements	<p>You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets.</p> <ul style="list-style-type: none"> • TCP invalid ACK check (the invalid-ack command) • TCP packet sequence past window check (the seq-past-window command) • TCP SYN-ACK with data check (the synack-data command) <p>You can also set the TCP out-of-order packet buffer timeout (the queue command timeout keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value.</p> <p>The default action for packets that exceed MSS has changed from drop to allow (the exceed-mss command).</p> <p>The following non-configurable actions have changed from drop to clear for these packet types:</p> <ul style="list-style-type: none"> • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option <p>In ASDM, see Configuration > Firewall > Objects > TCP Maps.</p>
TCP Intercept statistics	<p>You can enable collection for TCP Intercept statistics using the threat-detection statistics tcp-intercept command, and view them using the show threat-detection statistics command.</p> <p>In ASDM, see Configuration > Firewall > Threat Detection.</p>
Threat detection shun timeout	<p>You can now configure the shun timeout for threat detection using the threat-detection scanning-threat shun duration command.</p> <p>In ASDM, see Configuration > Firewall > Threat Detection.</p>
Threat detection host statistics fine tuning	<p>You can now reduce the amount of host statistics collected, thus reducing the system impact of this feature, by using the threat-detection statistics host number-of-rate command.</p> <p>In ASDM, see Configuration > Firewall > Threat Detection.</p>
Platform Features	
Increased VLANs	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.

New Features in Version 8.1(1)

Table 1-2 lists the new features for Version 8.1(1).



Note

Version 8.1(x) is only supported on the Cisco ASA 5580 adaptive security appliance.

Table 1-2 New Features for ASA Version 8.1(1)

Feature	Description
Introduction of the Cisco ASA 5580	<p>The Cisco ASA 5580 comes in two models:</p> <ul style="list-style-type: none"> • The ASA 5580-20 delivers 5 Gigabits per second of TCP traffic and UDP performance is even greater. Many features in the system have been made multi-core capable to achieve this high throughput. In addition the system delivers greater than 60,000 TCP connections per second and supports up to 1 million connections. • The ASA 5580-40 will deliver 10 Gigabits per second of TCP traffic and similar to ASA 5580-20 the UDP performance will be even greater. The ASA 5580-40 delivers greater than 120,000 TCP connections per second and up to 2 million connections in total. <p>In ASDM, see Home > System Resource Status and Home > Device Information > Environment Status.</p>
NetFlow	<p>The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. For detailed information on this feature and the new CLI commands, see the <i>Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide</i>.</p> <p>In ASDM, see Configuration > Device Management > Logging > Netflow.</p>
Timeout for SIP Provisional Media	<p>You can now configure the timeout for SIP provisional media using the timeout sip-provisional-media command.</p> <p>In ASDM, see Configuration > Firewall > Advanced > Global Timeouts.</p>
Details about the activation key	<p>You can now view the permanent and temporary activation keys with their enabled features, including all previously installed temporary keys and their expiration dates using the show activation key detail command.</p> <p>In ASDM in single context mode, see Configuration > Device Management > System Image/Configuration > Activation Key. In ASDM in multiple context mode, see System > Configuration > Device Management > Activation Key.</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 adaptive security appliance 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.

This section includes the following topics:

- [Security Policy Overview, page 1-6](#)
- [Firewall Mode Overview, page 1-8](#)
- [Stateful Inspection Overview, page 1-8](#)

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the adaptive security appliance 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. This section includes the following topics:

- [Permitting or Denying Traffic with Access Lists, page 1-6](#)
- [Applying NAT, page 1-6](#)
- [Protecting from IP Fragments, page 1-6](#)
- [Using AAA for Through Traffic, page 1-7](#)
- [Applying HTTP, HTTPS, or FTP Filtering, page 1-7](#)
- [Applying Application Inspection, page 1-7](#)
- [Applying QoS Policies, page 1-7](#)
- [Applying Connection Limits and TCP Normalization, page 1-7](#)

Permitting or Denying Traffic with Access Lists

You can apply an access list to limit traffic from inside to outside, or allow traffic from outside to inside. For transparent firewall mode, you can also apply an EtherType access list 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 adaptive security appliance 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 adaptive security appliance. Fragments that fail the security check are dropped and logged. Virtual reassembly cannot be disabled.

Using AAA for Through Traffic

You can require authentication and/or authorization for certain types of traffic, for example, for HTTP. The adaptive security appliance also sends accounting information to a RADIUS or TACACS+ server.

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. We recommend that you use the adaptive security appliance in conjunction with a separate server running one of the following Internet filtering products:

- Websense Enterprise
- Secure Computing SmartFilter

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 adaptive security appliance 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 adaptive security appliance 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 adaptive security appliance 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 adaptive security appliance to send system log messages about an attacker or you can automatically shun the host.

Firewall Mode Overview

The adaptive security appliance runs in two different firewall modes:

- Routed
- Transparent

In routed mode, the adaptive security appliance is considered to be a router hop in the network.

In transparent mode, the adaptive security appliance acts like a “bump in the wire,” or a “stealth firewall,” and is not considered a router hop. The adaptive security appliance connects to the same network on its inside and outside interfaces.

You might use a transparent firewall to simplify your network configuration. Transparent mode is also useful if you want the firewall to be invisible to attackers. You can also use a transparent firewall for traffic that would otherwise be blocked in routed mode. For example, a transparent firewall can allow multicast streams using an EtherType access list.

Stateful Inspection Overview

All traffic that goes through the adaptive security appliance 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.

A stateful firewall like the adaptive security appliance, however, takes into consideration the state of a packet:

- Is this a new connection?

If it is a new connection, the adaptive security appliance 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”



Note The session management path and the fast path make up the “accelerated security path.”

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 adaptive security appliance 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

For UDP or other connectionless protocols, the adaptive security appliance creates connection state information so that it can also use the fast path.

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 adaptive security appliance uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The adaptive security appliance 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 adaptive security appliance invokes various standard protocols to accomplish these functions.

The adaptive security appliance 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 adaptive security appliance invokes various standard protocols to accomplish these functions.

Security Context Overview

You can partition a single adaptive security appliance 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. Some features are not supported, including VPN and dynamic routing protocols.

In multiple context mode, the adaptive security appliance 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 adaptive security appliance. 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.

**Note**

You can run all your contexts in routed mode or transparent mode; you cannot run some contexts in one mode and others in another.

Multiple context mode supports static routing only.
