Introduction to the Security Appliance

The security appliance combines advanced stateful firewall and VPN concentrator functionality in one device, and for some models, an integrated intrusion prevention module called the AIP SSM or an integrated content security and control module called the CSC SSM. The 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 support, and many more features.

Note
ASDM 6.2(1) and higher is not supported on the PIX platforms. The last release that ASDM is supported on is 6.1(5).

This chapter includes the following sections:
- SSM and SSC Support Per Model, page 3-2
- VPN Specifications, page 3-2
- New Features, page 3-3
- Firewall Functional Overview, page 3-11
- VPN Functional Overview, page 3-19
- Security Context Overview, page 3-19
SSM and SSC Support Per Model

Table 3-1 shows the Security Services Modules (SSMs) and Security Services Cards (SSCs) supported by each platform:

<table>
<thead>
<tr>
<th>Platform</th>
<th>SSM Models</th>
<th>SSC Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5505</td>
<td>No support</td>
<td>AIP SSC 5</td>
</tr>
<tr>
<td>ASA 5510</td>
<td>AIP SSM 10</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>AIP SSM 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSC SSM 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSC SSM 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4GE SSM</td>
<td></td>
</tr>
<tr>
<td>ASA 5520</td>
<td>AIP SSM 10</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>AIP SSM 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIP SSM 40</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSC SSM 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSC SSM 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4GE SSM</td>
<td></td>
</tr>
<tr>
<td>ASA 5540</td>
<td>AIP SSM 10</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>AIP SSM 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIP SSM 40</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSC SSM 10^1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSC SSM 20^1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4GE SSM</td>
<td></td>
</tr>
<tr>
<td>ASA 5550</td>
<td>No support (the 4GE SSM is built-in and not user-removable)</td>
<td>No support</td>
</tr>
<tr>
<td>ASA 5580</td>
<td>No support</td>
<td>No support</td>
</tr>
</tbody>
</table>

1. The CSC SSM licenses support up to 1000 users while the Cisco ASA 5540 Series appliance can support significantly more users. If you deploy CSC SSM with an ASA 5540 adaptive security appliance, be sure to configure the security appliance to send the CSC SSM only the traffic that should be scanned.

VPN Specifications

# New Features

This section includes the following topics:

- New Features in ASDM 6.2(5)/ASA 8.2(2), page 3-3
- New Features in ASDM 6.2(3)/ASA 8.0(5), page 3-5
- New Features in ASDM 6.2(1)/ASA 8.2(1), page 3-6

## New Features in ASDM 6.2(5)/ASA 8.2(2)

**Released: January 11, 2010**

Table 3-2 lists the new features for ASA Version 8.2(2)/ASDM Version 6.2(5).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Access Features</strong></td>
<td></td>
</tr>
<tr>
<td>Scalable Solutions for Waiting-to-Resume VPN Sessions</td>
<td>An administrator can now keep track of the number of users in the active state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in. The following screen was modified: Monitoring &gt; VPN &gt; VPN Statistics &gt; Sessions. <em>Also available in Version 8.0(5).</em></td>
</tr>
</tbody>
</table>

| **Application Inspection Features** | |
| Inspection for IP Options | You can now control which IP packets with specific IP options should be allowed through the security appliance. You can also clear IP options from an IP packet, and then allow it through the security appliance. Previously, all IP options were denied by default, except for some special cases. **Note** This inspection is enabled by default. Therefore, the security appliance allows RSVP traffic that contains packets with the Router Alert option (option 20) when the security appliance is in routed mode. The following screens were introduced: Configuration > Firewall > Objects > Inspect Maps > IP-Options Configuration > Firewall > Service Policy > Add/Edit Service Policy Rule > Rule Actions > Protocol Inspection |

| Enabling Call Set up Between H.323 Endpoints | You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The security appliance includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint IP address is unknown and the security appliance opens a pinhole through source IP address/port 0/0. By default, this option is disabled. The following screen was modified: Configuration > Firewall > Objects > Inspect Maps > H.323 > Details > State Checking. *Also available in Version 8.0(5).* |

## Unified Communication Features
### New Features

**Mobility Proxy**

The Mobility Proxy no longer requires the UC Proxy license.

**Interface Features**

- In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements.
  - The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair.
  - The MAC addresses are also now persistent across reloads.
  - The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2.
  - The following screen was modified: Configuration > Context Management > Security Contexts. 
  - Also available in Version 8.0(5).

- Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces
  - You can now enable pause (XOFF) frames for flow control.
  - The following screens were modified:
    - (Single Mode) Configuration > Device Setup > Interfaces > Add/Edit Interface > General
    - (Multiple Mode, System) Configuration > Interfaces > Add/Edit Interface

**Firewall Features**

- Botnet Traffic Filter Enhancements
  - The Botnet Traffic Filter now supports automatic blocking of blacklisted traffic based on the threat level. You can also view the category and threat level of malware sites in statistics and reports. Reporting was enhanced to show infected hosts. The 1 hour timeout for reports for top hosts was removed; there is now no timeout.
  - The following screens were introduced or modified:
    - Configuration > Firewall > Botnet Traffic Filter > Traffic Settings
    - Monitoring > Botnet Traffic Filter > Infected Hosts

- Connection timeouts for all protocols
  - The idle timeout was changed to apply to all protocols, not just TCP.
  - The following screen was modified: Configuration > Firewall > Service Policies > Rule Actions > Connection Settings.

**Routing Features**

- DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues
  - This enhancement introduces security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each DHCP server configured for VPN clients, you can now configure the security appliance to send the Subnet Selection option or the Link Selection option.
  - The following screen was modified: Remote Access VPN > Network Access > IPsec connection profiles > Add/Edit.
  - Also available in Version 8.0(5).

### High Availability Features

---

Table 3-2  New Features for ASA Version 8.2(2)/ASDM Version 6.2(5) (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Proxy application no longer requires Unified Communications Proxy license</td>
<td>The Mobility Proxy no longer requires the UC Proxy license.</td>
</tr>
<tr>
<td>Interface Features</td>
<td></td>
</tr>
<tr>
<td>In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements</td>
<td>The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresses are also now persistent across reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2. The following screen was modified: Configuration &gt; Context Management &gt; Security Contexts. Also available in Version 8.0(5).</td>
</tr>
<tr>
<td>Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces</td>
<td>You can now enable pause (XOFF) frames for flow control. The following screens were modified: (Single Mode) Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface &gt; General (Multiple Mode, System) Configuration &gt; Interfaces &gt; Add/Edit Interface</td>
</tr>
<tr>
<td>Firewall Features</td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter Enhancements</td>
<td>The Botnet Traffic Filter now supports automatic blocking of blacklisted traffic based on the threat level. You can also view the category and threat level of malware sites in statistics and reports. Reporting was enhanced to show infected hosts. The 1 hour timeout for reports for top hosts was removed; there is now no timeout. The following screens were introduced or modified: Configuration &gt; Firewall &gt; Botnet Traffic Filter &gt; Traffic Settings Monitoring &gt; Botnet Traffic Filter &gt; Infected Hosts</td>
</tr>
<tr>
<td>Connection timeouts for all protocols</td>
<td>The idle timeout was changed to apply to all protocols, not just TCP. The following screen was modified: Configuration &gt; Firewall &gt; Service Policies &gt; Rule Actions &gt; Connection Settings.</td>
</tr>
<tr>
<td>Routing Features</td>
<td></td>
</tr>
<tr>
<td>DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues</td>
<td>This enhancement introduces security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each DHCP server configured for VPN clients, you can now configure the security appliance to send the Subnet Selection option or the Link Selection option. The following screen was modified: Remote Access VPN &gt; Network Access &gt; IPsec connection profiles &gt; Add/Edit. Also available in Version 8.0(5).</td>
</tr>
</tbody>
</table>

---
Table 3-2  New Features for ASA Version 8.2(2)/ASDM Version 6.2(5) (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Support in Failover Configurations</td>
<td>IPv6 is now supported in failover configurations. You can assign active and standby IPv6 addresses to interfaces and use IPv6 addresses for the failover and Stateful Failover interfaces. The following screens were modified: Configuration &gt; Device Management &gt; High Availability &gt; Failover &gt; Setup Configuration &gt; Device Management &gt; High Availability &gt; Failover &gt; Interfaces Configuration &gt; Device Management &gt; High Availability &gt; HA/Scalability Wizard</td>
</tr>
<tr>
<td>No notifications when interfaces are brought up or brought down during a switchover event</td>
<td>To distinguish between link up/down transitions during normal operation from link up/down transitions during failover, no link up/link down traps are sent during a failover. Also, no syslog messages about link up/down transitions during failover are sent. Also available in Version 8.0(5).</td>
</tr>
</tbody>
</table>

AAA Features

| 100 AAA Server Groups                  | You can now configure up to 100 AAA server groups; the previous limit was 15 server groups. The following screen was modified: Configuration > Device Management > Users/AAA > AAA Server Groups. |

Monitoring Features

| Smart Call Home                        | Smart Call Home offers proactive diagnostics and real-time alerts on the security appliance and provides higher network availability and increased operational efficiency. Customers and TAC engineers get what they need to resolve problems quickly when an issue is detected. Note Smart Call Home server Version 3.0(1) has limited support for the security appliance. See the “Important Notes” for more information. The following screen was introduced: Configuration > Device Management > Smart Call Home. |

New Features in ASDM 6.2(3)/ASA 8.0(5)

Released: November 3, 2009

Table 3-3 lists the new features for ASA Version 8.0(5)/ASDM Version 6.2(3).

Note Version 8.0(5) is not supported on the PIX security appliance.

Table 3-3  New Features for ASA Version 8.0(5)/ASDM Version 6.2(3)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access Features</td>
<td></td>
</tr>
<tr>
<td>Scalable Solutions for Waiting-to-Resume VPN Sessions</td>
<td>An administrator can now keep track of the number of users in the active state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in The following ASDM screen was modified: Monitoring &gt; VPN &gt; VPN Statistics &gt; Sessions. Also available in Version 8.2(2).</td>
</tr>
</tbody>
</table>

Application Inspection Features
Table 3-3  New Features for ASA Version 8.0(5)/ASDM Version 6.2(3) (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling Call Set up Between H.323 Endpoints</td>
<td>You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The</td>
</tr>
<tr>
<td></td>
<td>security appliance includes options to open pinholes for calls based on the RegistrationRequest/</td>
</tr>
<tr>
<td></td>
<td>RegistrationConfirm (RRQ/RCF) messages.</td>
</tr>
<tr>
<td></td>
<td>Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP</td>
</tr>
<tr>
<td></td>
<td>address is unknown and the security appliance opens a pinhole through source IP address/port 0/0.</td>
</tr>
<tr>
<td></td>
<td>By default, this option is disabled.</td>
</tr>
<tr>
<td></td>
<td>The following ASDM screen was modified: Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; H.323</td>
</tr>
<tr>
<td></td>
<td>&gt; Details &gt; State Checking.</td>
</tr>
<tr>
<td></td>
<td>Also available in Version 8.2(2).</td>
</tr>
<tr>
<td>Interface Features</td>
<td>The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2),</td>
</tr>
<tr>
<td></td>
<td>and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair.</td>
</tr>
<tr>
<td></td>
<td>The MAC addresses are also now persistent across reloads.</td>
</tr>
<tr>
<td></td>
<td>The command parser now checks if auto-generation is enabled; if you want to also manually assign a</td>
</tr>
<tr>
<td></td>
<td>MAC address, you cannot start the manual MAC address with A2.</td>
</tr>
<tr>
<td></td>
<td>The following ASDM screen was modified: Configuration &gt; Context Management &gt; Security Contexts.</td>
</tr>
<tr>
<td></td>
<td>Also available in Version 8.2(2).</td>
</tr>
<tr>
<td>High Availability Features</td>
<td>To distinguish between link up/down transitions during normal operation from link up/down transitions</td>
</tr>
<tr>
<td></td>
<td>during failover, no link up/link down traps are sent during a failover. Also, no syslog messages</td>
</tr>
<tr>
<td></td>
<td>about link up/down transitions during failover are sent.</td>
</tr>
<tr>
<td></td>
<td>Also available in Version 8.2(2).</td>
</tr>
<tr>
<td>Routing Features</td>
<td>This enhancement introduces security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection</td>
</tr>
<tr>
<td></td>
<td>Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). The following</td>
</tr>
<tr>
<td></td>
<td>ASDM screen was modified: Remote Access VPN &gt; Network Access &gt; IPsec connection profiles &gt; Add/Edit.</td>
</tr>
<tr>
<td></td>
<td>Also available in Version 8.2(2).</td>
</tr>
<tr>
<td>SSM Features</td>
<td>ASDM displays Web Reputation, User Group Policies, and User ID Settings in the Plus License listing</td>
</tr>
<tr>
<td></td>
<td>on the main home page. CSC 6.3 security event enhancements are included, such as the new Web</td>
</tr>
<tr>
<td></td>
<td>Reputation events and user and group identifications.</td>
</tr>
</tbody>
</table>

New Features in ASDM 6.2(1)/ASA 8.2(1)

Released: May 6, 2009
Table 3-4 lists the new features for ASA Version 8.2(1)/ASDM Version 6.2(1).

**Table 3-4 New Features for ASA Version 8.2(1)/ASDM Version 6.2(1)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Access Features</strong></td>
<td></td>
</tr>
<tr>
<td>One Time Password Support for ASDM Authentication</td>
<td>ASDM now supports administrator authentication using one time passwords (OTPs) supported by RSA SecurID (SDI). This feature addresses security concerns about administrators authenticating with static passwords. New session controls for ASDM users include the ability to limit the session time and the idle time. When the password used by the ASDM administrator times out, ASDM prompts the administrator to re-authenticate. In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; ASDM/HTTPD/Telnet/SSH.</td>
</tr>
<tr>
<td>Customizing Secure Desktop</td>
<td>You can use ASDM to customize the Secure Desktop windows displayed to remote users, including the Secure Desktop background (the lock icon) and its text color, and the dialog banners for the Desktop, Cache Cleaner, Keystroke Logger, and Close Secure Desktop windows. In ASDM, see Configuration &gt; CSD Manager &gt; Secure Desktop Manager.</td>
</tr>
<tr>
<td>Pre-fill Username from Certificate</td>
<td>The pre-fill username feature enables the use of a username extracted from a certificate for username/password authentication. With this feature enabled, the username is “pre-filled” on the login screen, with the user being prompted only for the password. The double-authentication feature is compatible with the pre-fill username feature, as the pre-fill username feature can support extracting a primary username and a secondary username from the certificate to serve as the usernames for double authentication when two usernames are required. In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect or Clientless SSL VPN Connection Profiles &gt; Advanced. Settings are in the Authentication, Secondary Authentication, and Authorization panes.</td>
</tr>
<tr>
<td>Double Authentication</td>
<td>The double authentication feature implements two-factor authentication for remote access to the network, in accordance with the Payment Card Industry Standards Council Data Security Standard. This feature requires that the user enter two separate sets of login credentials at the login page. For example, the primary authentication might be a one-time password, and the secondary authentication might be a domain (Active Directory) credential. If either authentication fails, the connection is denied. Both the AnyConnect VPN client and Clientless SSL VPN support double authentication. The AnyConnect client supports double authentication on Windows computers (including supported Windows Mobile devices and Start Before Logon), Mac computers, and Linux computers. The IPsec VPN client, SVC client, cut-through-proxy authentication, hardware client authentication, and management authentication do not support double authentication. <strong>Note</strong> The RSA/SDI authentication server type cannot be used as the secondary username/password credential. It can only be used for primary authentication. In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access or Clientless SSL VPN &gt; AnyConnect Connection Profiles &gt; Add/Edit &gt; Advanced &gt; Secondary Authentication.</td>
</tr>
</tbody>
</table>
### AnyConnect Essentials

AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the security appliance, that provides the full AnyConnect capability, with the following exceptions:

- No CSD (including HostScan/Vault/Cache Cleaner)
- No clientless SSL VPN
- Optional Windows Mobile Support

The AnyConnect Essentials client provides remote end users running Microsoft Windows Vista, Windows Mobile, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client.

**Note** This license cannot be used at the same time as the shared SSL VPN premium license.

In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials License. The AnyConnect Essentials license must be installed for ASDM to show this pane.

### Disabling Cisco Secure Desktop per Connection Profile

When enabled, Cisco Secure Desktop automatically runs on all computers that make SSL VPN connections to the security appliance. This new feature lets you exempt certain users from running Cisco Secure Desktop on a per connection profile basis. It prevents the detection of endpoint attributes for these sessions, so you might need to adjust the Dynamic Access Policy (DAP) configuration.

In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Add or Edit > Advanced, Clientless SSL VPN Configuration.

or

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add or Edit > Advanced > SSL VPN.

### Certificate Authentication Per Connection Profile

Previous versions supported certificate authentication for each security appliance interface, so users received certificate prompts even if they did not need a certificate. With this new feature, users receive a certificate prompt only if the connection profile configuration requires a certificate. This feature is automatic.

In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Basic.

or

Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profiles > Add/Edit>Basic.

### EKU Extensions for Certificate Mapping

This feature adds the ability to create certificate maps that look at the Extended Key Usage extension of a client certificate and use these values in determining what connection profile the client should use. If the client does not match that profile, it uses the default group. The outcome of the connection then depends on whether or not the certificate is valid and the authentication settings of the connection profile.

In ASDM, use the IPSec Certificate to Connection Maps > Rules pane, or Certificate to SSL VPN Connections Profile Maps pane.

### SSL VPN SharePoint Support for Win 2007 Server

Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.
### New Features

#### Shared license for SSL VPN sessions
You can purchase a shared license with a large number of SSL VPN sessions and share the sessions as needed among a group of security appliances by configuring one of the security appliances as a shared license server, and the rest as clients.

**Note** This license cannot be used at the same time as the AnyConnect Essentials license.

In ASDM, see Configuration > Device Management > Licensing > Shared SSL VPN Licenses. Also see, Monitoring > VPN > Clientless SSL VPN > Shared Licenses.

#### Updated VPN Wizard
The VPN Wizard (accessible by choosing Wizards > IPSec VPN Wizard) was updated. The step to select IPsec Encryption and Authentication (formerly Step 9 of 11) was removed because the Wizard now generates default values for these settings. In addition, the step to select IPsec Settings (Optional) now includes new fields to enable perfect forwarding secrecy (PFS) and set the Diffie-Hellman Group.

### Firewall Features

#### TCP state bypass
If you have asymmetric routing configured on upstream routers, and traffic alternates between two security appliances, then you can configure TCP state bypass for specific traffic.

In ASDM, see Configuration > Firewall > Service Policy Rules > Rule Actions > Connection Settings.

#### Per-Interface IP Addresses for the Media-Termination Instance Used by the Phone Proxy
In Version 8.0(4), you configured a global media-termination address (MTA) on the security appliance. In Version 8.2, you can now configure MTAs for individual interfaces (with a minimum of two MTAs). As a result of this enhancement, the old CLI has been deprecated. You can continue to use the old configuration if desired. However, if you need to change the configuration at all, only the new configuration method is accepted; you cannot later restore the old configuration.

In ASDM, see Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Media Termination Address.

#### H.239 Message Support in H.323 Application Inspection
In this release, the security appliance supports the H.239 standard as part of H.323 application inspection. H.239 is a standard that provides the ability for H.300 series endpoints to open an additional video channel in a single call. In a call, an endpoint (such as a video phone), sends a channel for video and a channel for data presentation. The H.239 negotiation occurs on the H.245 channel. The security appliance opens a pinhole for the additional media channel. The endpoints use open logical channel message (OLC) to signal a new channel creation. The message extension is part of H.245 version 13. The decoding and encoding of the telepresentation session is enabled by default. H.239 encoding and decoding is performed by ASN.1 coder.

In ASDM, see Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard > Rule Actions > Protocol Inspection > H.323 H.225. Click **Configure** and then choose the H.323 Inspect Map.

#### Processing H.323 Endpoints When the Endpoints Do Not Send OLCAck
H.323 application inspection has been enhanced to process common H.323 endpoints. The enhancement affects endpoints using the extendedVideoCapability OLC with the H.239 protocol identifier. Even when an H.323 endpoint does not send OLCAck after receiving an OLC message from a peer, the security appliance propagates OLC media proposal information into the media array and opens a pinhole for the media channel (extendedVideoCapability).

New Features

IPv6 in transparent firewall mode

Transparent firewall mode now participates in IPv6 routing. Prior to this release, the security appliance could not pass IPv6 traffic in transparent mode. You can now configure an IPv6 management address in transparent mode, create IPv6 access lists, and configure other IPv6 features; the security appliance recognizes and passes IPv6 packets.

All IPv6 functionality is supported unless specifically noted.

In ASDM, see Configuration > Device Management > Management Access > Management IP Address.

Botnet Traffic Filter

Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity. You can also supplement the dynamic database with a static database by entering IP addresses or domain names in a local “blacklist” or “whitelist.”

Note
This feature requires the Botnet Traffic Filter license. See the following licensing document for more information:


In ASDM, see Configuration > Firewall > Botnet Traffic Filter.

AIP SSC card for the ASA 5505

The AIP SSC offers IPS for the ASA 5505 security appliance. Note that the AIP SSM does not support virtual sensors.

In ASDM, see Configuration > Device Setup > SSC Setup and Configuration > IPS.

IPv6 support for IPS

You can now send IPv6 traffic to the AIP SSM or SSC when your traffic class uses the match any command, and the policy map specifies the ips command.

In ASDM, see Configuration > Firewall > Service Policy Rules.

Management Features

SNMP version 3 and encryption

This release provides DES, 3DES, or AES encryption and support for SNMP Version 3, the most secure form of the supported security models. This version allows you to configure authentication characteristics by using the User-based Security Model (USM).

In ASDM, see Configuration > Device Management > Management Access > SNMP.

NetFlow

This feature was introduced in Version 8.1(1) for the ASA 5580; this version introduces the feature to the other platforms. The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol.

In ASDM, see Configuration > Device Management > Logging > Netflow.

Routing Features

Multicast NAT

The security appliance now offers Multicast NAT support for group addresses.

Troubleshooting Features

Coredump functionality

A coredump is a snapshot of the running program when the program has terminated abnormally. Coredumps are used to diagnose or debug errors and save a crash for later or off-site analysis. Cisco TAC may request that users enable the coredump feature to troubleshoot application or system crashes on the security appliance.

To enable coredump, use the coredump enable command.
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 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:

- Configuring Public Servers, page 3-11
- Security Policy Overview, page 3-15
- Firewall Mode Overview, page 3-18
- Stateful Inspection Overview, page 3-18

### Configuring Public Servers

This section describes how to configure public servers, and includes the following topics:

- Public Server Overview, page 3-12
- Add a Public Server, page 3-12
- Edit a Public Server, page 3-14

### ASDM Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASDM Support for IPv6</strong></td>
<td>All IPv6 functionality is supported unless specifically noted.</td>
</tr>
<tr>
<td><strong>Support for Public Server configuration</strong></td>
<td>You can use ASDM to configure a public server. This allows you to define servers and services that you want to expose to an outside interface. In ASDM, see Configuration &gt; Firewall &gt; Public Servers.</td>
</tr>
</tbody>
</table>
Public Server Overview

While one of the basic functions of a firewall is to protect inside networks from unauthorized access by users on an outside network, or protect inside networks from each other, this function involves multiple configurations. That is, inside the DMZ interfaces, creating ACL lists and rules, NAT/PAT rules, and application inspection.

ASDM provides the Public Servers pane in the Configuration > Firewall > Public Servers pane, so that an administrator can publish various application servers to be accessed by internal and external users. When selected, this pane displays a list of public servers, internal and external addresses, the interfaces that the internal or external addresses apply to, and the service that is exposed.

In this pane you can add, edit, delete, or modify existing public servers.

Fields
- Add—Adds a public server.
- Edit—Edits a a public server group.
- Delete—Deletes a specified public server.
- Apply—Applies the changes that have been made.
- Reset—Resets the security appliance to the previous configuration.

Modes
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Add a Public Server

To add a public server, perform the following steps:

Note
STATIC PAT is not supported on a public server.

Step 1
In the Configuration > Firewall > Public Servers pane, click Add to add a new server.

The Add Public Server dialog box appears.

Step 2
Fill in the values of the Private Interface, Private IP Address, Service, Public Interface, and Public IP Address.

- Private Interface—Use the drop down menu to select the name of the private interface or enter the name in the field.
- Private IP Address—Click the ... browse button next to the Private IP address field to select the private IP address. The Browse Private IP Address dialog box appears.
• You can enter a name or Private IP address in the Filter field and click Filter. The wildcard characters asterisk (*) and question mark (?) are allowed. To delete the name you just typed, click Clear, or you can click Add. The Add Network Object dialog box appears.

**Step 3**
Fill in the following values in the Add Network Object dialog box:

- **Name**—(Optional) The object name. Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.
- **IP Address**—The IP address (host address).
- **Netmask**—The subnet mask for the IP address.
- **Description**—(Optional) The description of the network object.

**Step 4**
Click OK.

You can now use this network object when you create a rule. For an edited object, the change is inherited automatically by any rules using the object.

**Note**
You cannot delete a network object that is in use.

**Step 5**
Service—The service that is exposed to the outside. You can choose any of the currently defined services or a service group that has been created. Multiple services from various ports can be opened to the outside.

Click the ... browse button next to the Service address field to select the service. The Browse Service dialog box appears.

Browse Service Groups dialog box lets you choose a service group. This dialog box is used in multiple configuration windows, and is named appropriately for your current task.

**Step 6**
In the Browse Service Groups dialog box, choose the Service from the main menu, then click OK. Fill in the following values:

- **Public Interface**—Use the drop down menu to choose the name of the public interface or enter the name in the field.
- **Public IP Address**—The address of the server as seen from the outside. If IPv6 has been enabled, the list of IPv6 addresses will be visible from this list.
  Click the ... browse button next to the Public IP address field to choose the public IP address. The Browse Public IP Address dialog box appears.

**Step 7**
You can enter a name or Public IP address in the Filter field and click Filter. The wildcard characters asterisk (*) and question mark (?) are allowed. To delete the name you just typed, click Clear, or you can click Add. The Add Network Object dialog box appears.

**Step 8**
Fill in the following values from the Add Network Object dialog:

- **Name**—(Optional) The object name. Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.
- **IP Address**—The IP address (host address).
- **Netmask**—The subnet mask for the IP address.
- **Description**—(Optional) The description of the network object.

**Step 9**
Click OK.

You can now use this network object when you create a rule. For an edited object, the change is inherited automatically by any rules using the object.
Edit a Public Server

To configure a public server, perform the following steps:

**Step 1**  
In the Configuration > Firewall > Public Servers pane, click **Edit** to edit an object, or choose an existing public server and click **Edit**. The Edit Public Server dialog box appears.

**Step 2**  
Fill in the values of the Inside Interface, Inside Address, Service, Outside Interface, Outside Address by performing the following steps:

- **Private Interface** — Lists the inside interfaces that are currently defined and provides the interface where the server is located. Use the pulldown menu to select the name of the interface or enter the name in the field.
- **Private IP Address** — The address of the server as seen from the outside. If IPv6 has been enabled, the list of IPv6 addresses will be visible from this list. Click the ... browse button next to the Private IP Address field to select the private IP address. The Browse Private IP Address dialog box appears.
- **You can enter a name or inside IP address in the Filter field and click Filter. The wildcard characters asterisk (*) and question mark (?) are allowed. To delete the name you just typed, click Clear, or you can click Add. The Add Network Object dialog box appears.**

**Step 3**  
Fill in the following values from the Add Network Object dialog:

- **Name** — (Optional) The object name. Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.
- **IP Address** — The IP address (host address).
- **Netmask** — The subnet mask for the IP address.
- **Description** — (Optional) The description of the network object.

**Step 4**  
Click OK.

You can now use this network object when you create a rule. For an edited object, the change is inherited automatically by any rules using the object.

**Note**  
You cannot delete a network object that is in use.
**Step 5**  Service—The service that is exposed to the outside. You can choose any of the currently defined services or a service group that has been created. Multiple services from various ports can be opened to the outside.

Click the ... browse button next to the Service address field to choose the service.

The Browse Service dialog box appears.

Browse Service Groups dialog box lets you choose a service group. This dialog box is used in multiple configuration screens and is named appropriately for your current task.

**Step 6**  On the Browse Service Groups dialog box, choose the Service from the main menu, then click OK.

- Public Interface—A drop down list that displays the interfaces that are currently defined and allows you to specify which interface has access to the server.

  Use the pulldown menu to select the name of the outside interface or enter the name in the field.

- Public IP Address—Click the ... browse button next to the Public IP Address field to select the outside IP address. The Browse IP Address dialog box appears.

- You can enter a name or IP address in the Filter field and click Filter. The wildcard characters asterisk (*) and question mark (?) are allowed. To delete the name you just typed, click **Clear**, or you can click Add. The Add Network Object dialog box appears.

**Step 7**  Fill in the following values from the Add Network Object dialog:

- Name—(Optional) The object name. Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.

- IP Address—The IP address (host address).

- Netmask—The subnet mask for the IP address.

- Description—(Optional) The description of the network object.

**Step 8**  Click OK.

You can now use this network object when you create a rule. For an edited object, the change is inherited automatically by any rules using the object.

---

**Security Policy Overview**

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the 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 3-16
- Applying NAT, page 3-16
- Protecting from IP Fragments, page 3-16
- Using AAA for Through Traffic, page 3-16
- Applying HTTP, HTTPS, or FTP Filtering, page 3-16
- Applying Application Inspection, page 3-16
- Sending Traffic to the Advanced Inspection and Prevention Security Services Module, page 3-17
- Sending Traffic to the Content Security and Control Security Services Module, page 3-17
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 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 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 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 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 security appliance to perform a deep packet inspection.
Sending Traffic to the Advanced Inspection and Prevention Security Services Module

If your model supports the AIP SSM for intrusion prevention, then you can send traffic to the AIP SSM for inspection. The AIP SSM is an intrusion prevention services module that monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. Other legitimate connections continue to operate independently without interruption. For more information, see Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface.

Sending Traffic to the Content Security and Control Security Services Module

If your model supports it, the CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that you configure the security appliance to send to it.

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

The security appliance runs in two different firewall modes:

- Routed
- Transparent

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

In transparent mode, the security appliance acts like a “bump in the wire,” or a “stealth firewall,” and is not considered a router hop. The 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 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 security appliance, however, takes into consideration the state of a packet:

- Is this a new connection?
  
  If it is a new connection, the 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 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
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 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 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 security appliance invokes various standard protocols to accomplish these functions.

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

Security Context Overview

You can partition a single 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 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 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.