



# Cisco ASA New Features by Release

---

**Updated: January 7, 2014**

This document lists new features by ASA release, and includes the following sections:

- [New Features in Version 9.1, page 1](#)
- [New Features in Version 9.0, page 13](#)
- [New Features in Version 8.7, page 31](#)
- [New Features in Version 8.6, page 33](#)
- [New Features in Version 8.5, page 36](#)
- [New Features in Version 8.4, page 40](#)
- [New Features in Version 8.3, page 70](#)
- [New Features in Version 8.2, page 80](#)
- [New Features in Version 8.1, page 98](#)
- [New Features in Version 8.0, page 103](#)
- [New Features in Version 7.2, page 121](#)
- [New Features in Version 7.1, page 141](#)
- [New Features in Version 7.0, page 148](#)



**Note**

---

New, changed, and deprecated syslog messages are listed in the syslog message guide for your release.

---

## New Features in Version 9.1

This section includes the following topics:

- [New Features in ASA 9.1\(4\)/ASDM 7.1\(5\), page 2](#)
- [New Features in ASA 9.1\(3\)/ASDM 7.1\(4\), page 4](#)
- [New Features in ASA 9.1\(2\)/ASDM 7.1\(3\), page 5](#)
- [New Features in ASA 9.1\(1\)/ASDM 7.1\(1\), page 12](#)



---

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

## New Features in ASA 9.1(4)/ASDM 7.1(5)

Released: December 9, 2013

Table 1 lists the new features for ASA Version 9.1(4)/ASDM Version 7.1(5).

**Table 1** *New Features for ASA Version 9.1(4)/ASDM Version 7.1(5)*

Feature	Description
<b>Remote Access Features</b>	
HTML5 WebSocket proxying	<p>HTML5 WebSockets provide persistent connections between clients and servers. During the establishment of the clientless SSL VPN connection, the handshake appears to the server as an HTTP Upgrade request. The ASA will now proxy this request to the backend and provide a relay after the handshake is complete. Gateway mode is not currently supported.</p> <p>We did not modify any commands.</p> <p>We did not modify any ASDM screens.</p>
Inner IPv6 for IKEv2	<p>IPv6 traffic can now be tunneled through IPsec/IKEv2 tunnels. This makes the ASA to AnyConnect VPN connections fully IPv6 compliant. GRE is used when both IPv4 and IPv6 traffic are being tunneled, and when both the client and headend support GRE. For a single traffic type, or when GRE is not supported by the client or the headend, we use straight IPsec.</p> <p><b>Note</b> This feature requires AnyConnect Client Version 3.1.05 or later.</p> <p>Output of the <b>show ipsec sa</b> and <b>show vpn-sessiondb detail anyconnect</b> commands has been updated to reflect the assigned IPv6 address, and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic.</p> <p>The <b>vpn-filter</b> command must now be used for both IPv4 and IPv6 ACLs. If the deprecated <b>ipv6-vpn-filter</b> command is used to configure IPv6 ACLs the connection will be terminated.</p> <p>We did not modify any ASDM screens.</p>
Mobile Devices running Citrix Server Mobile have additional connection options	<p>Support for mobile devices connecting to Citrix server through the ASA now includes selection of a tunnel-group, and RSA Securid for authorization. Allowing mobile users to select different tunnel-groups allows the administrator to use different authentication methods.</p> <p>We introduced the <b>application-type</b> command to configure the default tunnel group for VDI connections when a Citrix Receiver user does not choose a tunnel-group. A <b>none</b> action was added to the <b>vdj</b> command to disable VDI configuration for a particular group policy or user.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; VDI Access.</p>
Split-tunneling supports exclude ACLs	<p>Split-tunneling of VPN traffic has been enhanced to support both exclude and include ACLs. Exclude ACLs were previously ignored.</p> <p><b>Note</b> This feature requires AnyConnect Client Version 3.1.03103 or later.</p> <p>We did not modify any commands.</p> <p>We did not modify any ASDM screens.</p>
<b>High Availability and Scalability Features</b>	

**Table 1**      **New Features for ASA Version 9.1(4)/ASDM Version 7.1(5) (continued)**

Feature	Description
ASA 5500-X support for clustering	<p>The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now support 2-unit clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 5512-X, you need the Security Plus license.</p> <p>We did not modify any commands.</p> <p>We did not modify any ASDM screens.</p>
Improved VSS and vPC support for health check monitoring	<p>If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, you can now increase stability with health check monitoring. For some switches, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable the VSS/vPC health check feature, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them.</p> <p>We modified the following command: <b>health-check [vss-enabled]</b></p> <p>We modified the following screen: Configuration &gt; Device Management &gt; High Availability and Scalability &gt; ASA Cluster</p>
Support for cluster members at different geographical locations (inter-site); Individual Interface mode only	<p>You can now place cluster members at different geographical locations when using individual interface mode. See the configuration guide for inter-site guidelines.</p> <p>We did not modify any commands.</p> <p>We did not modify any ASDM screens.</p>
<b>Basic Operation Features</b>	
DHCP rebind function	<p>During the DHCP rebind phase, the client now attempts to rebind to other DHCP servers in the tunnel group list. Prior to this release, the client did not rebind to an alternate server, when the DHCP lease fails to renew.</p> <p>We introduced the following commands: <b>show ip address dhcp lease proxy</b>, <b>show ip address dhcp lease summary</b>, and <b>show ip address dhcp lease server</b>.</p> <p>We introduced the following screen: Monitoring &gt; Interfaces &gt; DHCP&gt; DHCP Lease Information.</p>
<b>Troubleshooting Features</b>	
Crashinfo dumps include AK47 framework information	<p>Application Kernel Layer 4 to 7 (AK47) framework-related information is now available in crashinfo dumps. A new option, <b>ak47</b>, has been added to the <b>debug menu</b> command to help in debugging AK47 framework issues. The framework-related information in the crashinfo dump includes the following:</p> <ul style="list-style-type: none"> <li>• Creating an AK47 instance.</li> <li>• Destroying an AK47 instance.</li> <li>• Generating a crashinfo with a memory manager frame.</li> <li>• Generating a crashinfo after fiber stack overflow.</li> <li>• Generating a crashinfo after a local variable overflow.</li> <li>• Generating a crashinfo after an exception has occurred.</li> </ul>

## New Features in ASA 9.1(3)/ASDM 7.1(4)

Released: September 18, 2013

Table 20 lists the new features for ASA Version 9.1(3)/ASDM Version 7.1(4).

**Table 2**      **New Features for ASA Version 9.1(3)/ASDM Version 7.1(4)**

Feature	Description
<b>Module Features</b>	
Support for the ASA CX module in multiple context mode	<p>You can now configure ASA CX service policies per context on the ASA.</p> <p><b>Note</b> Although you can configure per context ASA service policies, the ASA CX module itself (configured in PRSM) is a single context mode device; the context-specific traffic coming from the ASA is checked against the common ASA CX policy.</p> <p>Requires ASA CX 9.2(1) or later.</p> <p>We did not modify any commands.</p> <p>We did not modify any ASDM screens.</p>
ASA 5585-X with SSP-40 and -60 support for the ASA CX SSP-40 and -60	<p>ASA CX SSP-40 and -60 modules can be used with the matching level ASA 5585-X with SSP-40 and -60.</p> <p>Requires ASA CX 9.2(1) or later.</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p>
Filtering packets captured on the ASA CX backplane	<p>You can now filter packets that have been captured on the ASA CX backplane using the <b>match</b> or <b>access-list</b> keyword with the <b>capture interface asa_dataplane</b> command. Control traffic specific to the ASA CX module is not affected by the access-list or match filtering; the ASA captures all control traffic. In multiple context mode, configure the packet capture per context. Note that all control traffic in multiple context mode goes only to the system execution space. Because only control traffic cannot be filtered using an access list or match, these options are not available in the system execution space.</p> <p>Requires ASA CX 9.2(1) or later.</p> <p>We modified the following command: <b>capture interface asa_dataplane</b>.</p> <p>A new option, Use backplane channel, was added to the Ingress Traffic Selector screen and the Egress Selector screen, in the Packet Capture Wizard to enable filtering of packets that have been captured on the ASA CX backplane.</p>
<b>Monitoring Features</b>	
Ability to view top 10 memory users	<p>You can now view the top bin sizes allocated and the top 10 PCs for each allocated bin size. Previously, you had to enter multiple commands to see this information (the <b>show memory detail</b> command and the <b>show memory binsize</b> command); the new command provides for quicker analysis of memory issues.</p> <p>We introduced the following command: <b>show memory top-usage</b>.</p> <p>We did not modify any ASDM screens.</p> <p><i>Also available in 8.4(6).</i></p>

**Table 2**      **New Features for ASA Version 9.1(3)/ASDM Version 7.1(4) (continued)**

Feature	Description
Smart Call Home	<p>We added a new type of Smart Call Home message to support ASA clustering.</p> <p>A Smart Call Home clustering message is sent for only the following three events:</p> <ul style="list-style-type: none"> <li>• When a unit joins the cluster</li> <li>• When a unit leaves the cluster</li> <li>• When a cluster unit becomes the cluster master</li> </ul> <p>Each message that is sent includes the following information:</p> <ul style="list-style-type: none"> <li>• The active cluster member count</li> <li>• The output of the <b>show cluster info</b> command and the <b>show cluster history</b> command on the cluster master</li> </ul> <p>We modified the following commands: <b>show call-home</b>, <b>show running-config call-home</b>.</p> <p>We did not modify any ASDM screens.</p> <p><i>Also available in 9.0(3).</i></p>
<b>Remote Access Features</b>	
<b>user-storage value</b> command password is now encrypted in <b>show</b> commands	<p>The password in the <b>user-storage value</b> command is now encrypted when you enter <b>show running-config</b>.</p> <p>We modified the following command: <b>user-storage value</b>.</p> <p>We modified the following screen: <b>Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Group Policies &gt; More Options &gt; Session Settings</b>.</p> <p><i>Also available in 8.4(6).</i></p>

## New Features in ASA 9.1(2)/ASDM 7.1(3)

**Released: May 14, 2013**

[Table 3](#) lists the new features for ASA Version 9.1(2)/ASDM Version 7.1(3).



### Note

Features added in 8.4(6) are not included in 9.1(2) unless they are explicitly listed in this table.

**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3)**

Feature	Description
<b>Certification Features</b>	
FIPS and Common Criteria certifications	<p>The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 FIPS 140-2 validation for the Cisco ASA series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X, and the ASA Services Module.</p> <p>The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which provides the basis for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform solutions.</p>

**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)**

Feature	Description
<b>Encryption Features</b>	
Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications	<p>Instead of using the proprietary encryption for the failover key (the <b>failover key</b> command), you can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption.</p> <p><b>Note</b> Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.</p> <p>We introduced or modified the following commands: <b>failover ipsec pre-shared-key</b>, <b>show vpn-sessiondb</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; High Availability &gt; Failover &gt; Setup.</p>
Additional ephemeral Diffie-Hellman ciphers for SSL encryption	<p>The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher suites:</p> <ul style="list-style-type: none"> <li>DHE-AES128-SHA1</li> <li>DHE-AES256-SHA1</li> </ul> <p>These cipher suites are specified in RFC 3268, <i>Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)</i>.</p> <p>When supported by the client, DHE is the preferred cipher because it provides Perfect Forward Secrecy. See the following limitations:</p> <ul style="list-style-type: none"> <li>DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS 1.0 for the SSL server.</li> </ul> <pre>!! set server version hostname(config)# <b>ssl server-version tlsv1 sslv3</b> !! set client version hostname(config) # <b>ssl client-version any</b></pre> <ul style="list-style-type: none"> <li>Some popular applications do not support DHE, so include at least one other SSL encryption method to ensure that a cipher suite common to both the SSL client and server can be used.</li> <li>Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Secure Desktop, and Internet Explorer 9.0.</li> </ul> <p>We modified the following command: <b>ssl encryption</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Advanced &gt; SSL Settings.</p> <p><i>Also available in 8.4(4.1).</i></p>
<b>Management Features</b>	

**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)**

Feature	Description
Support for administrator password policy when using the local database	<p>When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters.</p> <p>We introduced the following commands: <b>change-password</b>, <b>password-policy lifetime</b>, <b>password-policy minimum changes</b>, <b>password-policy minimum-length</b>, <b>password-policy minimum-lowercase</b>, <b>password-policy minimum-uppercase</b>, <b>password-policy minimum-numeric</b>, <b>password-policy minimum-special</b>, <b>password-policy authenticate enable</b>, <b>clear configure password-policy</b>, <b>show running-config password-policy</b>.</p> <p>We introduced the following screen: Configuration &gt; Device Management &gt; Users/AAA &gt; Password Policy.</p> <p><i>Also available in 8.4(4.1).</i></p>
Support for SSH public key authentication	<p>You can now enable public key authentication for SSH connections to the ASA on a per-user basis. You can specify a public key file (PKF) formatted key or a Base64 key. The PKF key can be up to 4096 bits. Use PKF format for keys that are too large to for the ASA support of the Base64 format (up to 2048 bits).</p> <p>We introduced the following commands: <b>ssh authentication</b>.</p> <p>We introduced the following screens:</p> <p>Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts &gt; Edit User Account &gt; Public Key Authentication</p> <p>Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts &gt; Edit User Account &gt; Public Key Using PKF</p> <p><i>Also available in 8.4(4.1); PKF key format support is only in 9.1(2).</i></p>
AES-CTR encryption for SSH	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
Improved SSH rekey interval	<p>An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic.</p> <p>We introduced the following command: <b>show ssh sessions detail</b>.</p>
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	<p>Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported.</p> <p>We introduced the following command: <b>ssh key-exchange</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Management Access &gt; ASDM/HTTPS/Telnet/SSH.</p> <p><i>Also available in 8.4(4.1).</i></p>
Support for a maximum number of management sessions	<p>You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions.</p> <p>We introduced the following commands: <b>quota management-session</b>, <b>show running-config quota management-session</b>, <b>show quota management-session</b>.</p> <p>We introduced the following screen: Configuration &gt; Device Management &gt; Management Access &gt; Management Session Quota.</p> <p><i>Also available in 8.4(4.1).</i></p>

**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)**

Feature	Description
Support for a pre-login banner in ASDM	Administrator can define a message that appears before a user logs into ASDM for management access. This customizable content is called a pre-login banner, and can notify users of special requirements or important information.
The default Telnet password was removed	<p>To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. <b>Note:</b> The login password is only used for Telnet if you do not configure Telnet user authentication (the <b>aaa authentication telnet console</b> command).</p> <p>Formerly, when you cleared the password, the ASA restored the default of “cisco.” Now when you clear the password, the password is removed.</p> <p>The login password is also used for Telnet sessions from the switch to the ASASM (see the <b>session</b> command). For initial ASASM access, you must use the <b>service-module session</b> command, until you set a login password.</p> <p>We modified the following command: <b>passwd</b>.</p> <p>We did not modify any ASDM screens.</p> <p><i>Also available in 9.0(2).</i></p>
<b>Platform Features</b>	
Support for Power-On Self-Test (POST)	<p>The ASA runs its power-on self-test at boot time even if it is not running in FIPS 140-2-compliant mode.</p> <p>Additional tests have been added to the POST to address the changes in the AES-GCM/GMAC algorithms, ECDSA algorithms, PRNG, and Deterministic Random Bit Generator Validation System (DRBGVS).</p>
Improved pseudo-random number generation (PRNG)	The X9.31 implementation has been upgraded to use AES-256 encryption instead of 3DES encryption to comply with the Network Device Protection Profile (NDPP) in single-core ASAs.
Support for image verification	<p>Support for SHA-512 image integrity checking was added.</p> <p>We modified the following command: <b>verify</b>.</p> <p>We did not modify any ASDM screens.</p> <p><i>Also available in 8.4(4.1).</i></p>
Support for private VLANs on the ASA Services Module	You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information.
CPU profile enhancements	<p>The <b>cpu profile activate</b> command now supports the following:</p> <ul style="list-style-type: none"> <li>• Delayed start of the profiler until triggered (global or specific thread CPU%)</li> <li>• Sampling of a single thread</li> </ul> <p>We modified the following command: <b>cpu profile activate</b> [<i>n-samples</i>] [<b>sample-process</b> <i>process-name</i>] [<b>trigger cpu-usage</b> <i>cpu%</i>] [<i>process-name</i>].</p> <p>We did not modify any ASDM screens.</p> <p><i>Also available in 8.4(6).</i></p>
<b>DHCP Features</b>	



**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)**

Feature	Description
DHCP relay servers per interface (IPv4 only)	<p>You can now configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. IPv6 is not supported for per-interface DHCP relay.</p> <p>We introduced or modified the following commands: <b>dhcprelay server</b> (interface config mode), <b>clear configure dhcprelay</b>, <b>show running-config dhcprelay</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Relay.</p>
DHCP trusted interfaces	<p>You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface.</p> <p>We introduced or modified the following commands: <b>dhcprelay information trusted</b>, <b>dhcprelay informarion trust-all</b>, <b>show running-config dhcprelay</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Relay.</p>
<b>Module Features</b>	
ASA 5585-X support for network modules	<p>The ASA 5585-X now supports additional interfaces on network modules in slot 1. You can install one or two of the following optional network modules:</p> <ul style="list-style-type: none"> <li>• ASA 4-port 10G Network Module</li> <li>• ASA 8-port 10G Network Module</li> <li>• ASA 20-port 1G Network Module</li> </ul> <p><i>Also available in 8.4(4.1).</i></p>
ASA 5585-X DC power supply support	<p>Support was added for the ASA 5585-X DC power supply.</p> <p><i>Also available in 8.4(5).</i></p>
Support for ASA CX monitor-only mode for demonstration purposes	<p>For demonstration purposes only, you can enable monitor-only mode for the service policy, which forwards a copy of traffic to the ASA CX module, while the original traffic remains unaffected.</p> <p>Another option for demonstration purposes is to configure a traffic-forwarding interface instead of a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic directly to the ASA CX module, bypassing the ASA.</p> <p>We modified or introduced the following commands: <b>cxsc {fail-close   fail-open} monitor-only</b>, <b>traffic-forward cxsc monitor-only</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule &gt; Rule Actions &gt; ASA CX Inspection.</p> <p>The traffic-forwarding feature is supported by CLI only.</p>
Support for the ASA CX module and NAT 64	<p>You can now use NAT 64 in conjunction with the ASA CX module.</p> <p>We did not modify any commands.</p> <p>We did not modify any ASDM screens.</p>

**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)**

Feature	Description
<b>NetFlow Features</b>	
Support for NetFlow flow-update events and an expanded set of NetFlow templates	<p>In addition to adding the flow-update events, there are now NetFlow templates that allow you to track flows that experience a change to their IP version with NAT, as well as IPv6 flows that remain IPv6 after NAT.</p> <p>Two new fields were added for IPv6 translation support.</p> <p>Several NetFlow field IDs were changed to their IPFIX equivalents.</p> <p>For more information, see the <i>Cisco ASA Implementation Note for NetFlow Collectors</i>.</p>
<b>Firewall Features</b>	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	<p>In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL.</p> <p>We modified the following command: <b>access-list ethertype {permit   deny} is-is</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Management Access &gt; EtherType Rules.</p> <p><i>Also available in 8.4(5).</i></p>
Decreased the half-closed timeout minimum value to 30 seconds	<p>The half-closed timeout minimum value for both the global timeout and connection timeout was lowered from 5 minutes to 30 seconds to provide better DoS protection.</p> <p>We modified the following commands: <b>set connection timeout half-closed, timeout half-closed</b>.</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; Service Policy Rules &gt; Connection Settings</p> <p>Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</p>
<b>Remote Access Features</b>	
IKE security and performance improvements	<p>The number of IPsec-IKE security associations (SAs) can be limited for IKE v1 now, as well as IKE v2.</p> <p>We modified the following command: <b>crypto ikev1 limit</b>.</p> <p>We modified the following screen: Configuration &gt; Site-to-Site VPN &gt; Advanced &gt; IKE Parameters.</p>
	<p>The IKE v2 Nonce size has been increased to 64 bytes.</p> <p>There are no ASDM screen or CLI changes.</p>
	<p>For IKE v2 on Site-to-Site, a new algorithm ensures that the encryption algorithm used by child IPsec SAs is not higher strength than the parent IKE. Higher strength algorithms will be downgraded to the IKE level.</p> <p>This new algorithm is enabled by default. We recommend that you do not disable this feature.</p> <p>We introduced the following command: <b>crypto ipsec ikev2 sa-strength-enforcement</b>.</p> <p>We did not modify any ASDM screens.</p>
	<p>For Site-to-Site, IPsec data-based rekeying can be disabled.</p> <p>We modified the following command: <b>crypto ipsec security-association</b>.</p> <p>We modified the following screen: Configuration &gt; Site-to-Site &gt; IKE Parameters.</p>

**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)**

Feature	Description
Improved Host Scan and ASA Interoperability	<p>Host Scan and the ASA use an improved process to transfer posture attributes from the client to the ASA. This gives the ASA more time to establish a VPN connection with the client and apply a dynamic access policy.</p> <p><i>Also available in 8.4(5).</i></p>
Clientless SSL VPN: Windows 8 Support	<p>This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems.</p> <p>We support the following browsers on Windows 8:</p> <ul style="list-style-type: none"> <li>• Internet Explorer 10 (desktop only)</li> <li>• Firefox (all supported Windows 8 versions)</li> <li>• Chrome (all supported Windows 8 versions)</li> </ul> <p>See the following limitations:</p> <ul style="list-style-type: none"> <li>• Internet Explorer 10: <ul style="list-style-type: none"> <li>– The Modern (AKA Metro) browser is not supported.</li> <li>– If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone.</li> <li>– If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported.</li> </ul> </li> <li>• A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported.</li> </ul> <p><i>Also available in 9.0(2).</i></p>
Cisco Secure Desktop: Windows 8 Support	<p>CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check.</p> <p>See the following limitations:</p> <ul style="list-style-type: none"> <li>• Secure Desktop (Vault) is not supported with Windows 8.</li> </ul> <p><i>Also available in 9.0(2).</i></p>
Dynamic Access Policies: Windows 8 Support	<p>ASDM was updated to enable selection of Windows 8 in the DAP Operating System attribute.</p> <p><i>Also available in 9.0(2).</i></p>
<b>Monitoring Features</b>	

**Table 3**      **New Features for ASA Version 9.1(2)/ASDM Version 7.1(3) (continued)**

Feature	Description
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP.  This data is equivalent to the <b>show xlate count</b> command.  We did not modify any ASDM screens.  <i>Also available in 8.4(5).</i>
NSEL	Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent.  We introduced or modified the following commands: <b>flow-export active refresh-interval</b> , <b>flow-export event-type</b> .  We modified the following screens:  Configuration > Device Management > Logging > NetFlow. Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard - Rule Actions > NetFlow > Add Flow Event  <i>Also available in 8.4(5).</i>

## New Features in ASA 9.1(1)/ASDM 7.1(1)

**Released: December 3, 2012**

[Table 17](#) lists the new features for ASA Version 9.1(1)/ASDM Version 7.1(1).



**Note**

Features added in 8.4(4.x), 8.4(5), 8.4(6), and 9.0(2) are not included in 9.1(1) unless they were listed in the 9.0(1) feature table.

**Table 4**      **New Features for ASA Version 9.1(1)/ASDM Version 7.1(1)**

Feature	Description
<b>Module Features</b>	
Support for the ASA CX SSP for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA CX SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. The ASA CX software module requires a Cisco solid state drive (SSD) on the ASA. For more information about the SSD, see the ASA 5500-X hardware guide.  We modified the following commands: <b>session cxsc</b> , <b>show module cxsc</b> , <b>sw-module cxsc</b> .  We did not modify any screens.

## New Features in Version 9.0

This section includes the following topics:

- [New Features in ASA 9.0\(3\)/ASDM 7.1\(3\), page 13](#)
- [New Features in ASA 9.0\(2\)/ASDM 7.1\(2\), page 13](#)
- [New Features in ASA 9.0\(1\)/ASDM 7.0\(1\), page 14](#)

### New Features in ASA 9.0(3)/ASDM 7.1(3)

**Released: July 22, 2013**

[Table 6](#) lists the new features for ASA Version 9.0(3)/ASDM Version 7.1(3).



**Note**

Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(3) unless they were listed in the 9.0(1) feature table.

**Table 5**      ***New Features for ASA Version 9.0(3)/ASDM Version 7.1(3)***

Feature	Description
<b>Monitoring Features</b>	
Smart Call Home	<p>We added a new type of Smart Call Home message to support ASA clustering. A Smart Call Home clustering message is sent for only the following three events:</p> <ul style="list-style-type: none"> <li>• When a unit joins the cluster</li> <li>• When a unit leaves the cluster</li> <li>• When a cluster unit becomes the cluster master</li> </ul> <p>Each message that is sent includes the following information:</p> <ul style="list-style-type: none"> <li>• The active cluster member count</li> <li>• The output of the <b>show cluster info</b> command and the <b>show cluster history</b> command on the cluster master</li> </ul>

### New Features in ASA 9.0(2)/ASDM 7.1(2)

**Released: February 25, 2013**

[Table 6](#) lists the new features for ASA Version 9.0(2)/ASDM Version 7.1(2).



**Note**

Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(2) unless they were listed in the 9.0(1) feature table.

**Table 6** *New Features for ASA Version 9.0(2)/ASDM Version 7.1(2)*

Feature	Description
<b>Remote Access Features</b>	
Clientless SSL VPN: Windows 8 Support	<p>This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems.</p> <p>We support the following browsers on Windows 8:</p> <ul style="list-style-type: none"> <li>• Internet Explorer 10 (desktop only)</li> <li>• Firefox (all supported Windows 8 versions)</li> <li>• Chrome (all supported Windows 8 versions)</li> </ul> <p>See the following limitations:</p> <ul style="list-style-type: none"> <li>• Internet Explorer 10: <ul style="list-style-type: none"> <li>– The Modern (AKA Metro) browser is not supported.</li> <li>– If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone.</li> <li>– If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported.</li> </ul> </li> <li>• A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported.</li> </ul>
Cisco Secure Desktop: Windows 8 Support	<p>CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check.</p> <p>See the following limitations:</p> <ul style="list-style-type: none"> <li>• Secure Desktop (Vault) is not supported with Windows 8.</li> </ul>
Dynamic Access Policies: Windows 8 Support	<p>ASDM was updated to enable selection of Windows 8 in the DAP Operating System attribute.</p>
<b>Management Features</b>	
The default Telnet password was removed	<p>To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. <b>Note:</b> The login password is only used for Telnet if you do not configure Telnet user authentication (the <b>aaa authentication telnet console</b> command).</p> <p>Formerly, when you cleared the password, the ASA restored the default of “cisco.” Now when you clear the password, the password is removed.</p> <p>The login password is also used for Telnet sessions from the switch to the ASASM (see the <b>session</b> command). For initial ASASM access, you must use the <b>service-module session</b> command, until you set a login password.</p> <p>We modified the following command: <b>passwd</b>.</p> <p>We did not modify any ASDM screens.</p>

## New Features in ASA 9.0(1)/ASDM 7.0(1)

**Released: October 29, 2012**

Table 17 lists the new features for ASA Version 9.0(1)/ASDM Version 7.0(1).



**Note**

Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(1) unless they are explicitly listed in this table.

**Table 7**      **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1)**

Feature	Description
<b>Firewall Features</b>	
Cisco TrustSec integration	<p>Cisco TrustSec provides an access-control solution that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec solution, enforcement devices utilize a combination of user attributes and end-point attributes to make role-based and identity-based access control decisions.</p> <p>In this release, the ASA integrates with Cisco TrustSec to provide security group based policy enforcement. Access policies within the Cisco TrustSec domain are topology-independent, based on the roles of source and destination devices rather than on network IP addresses.</p> <p>The ASA can utilize the Cisco TrustSec solution for other types of security group based policies, such as application inspection; for example, you can configure a class map containing an access policy based on a security group.</p> <p>We introduced or modified the following commands: <b>access-list extended</b>, <b>cts sxp enable</b>, <b>cts server-group</b>, <b>cts sxp default</b>, <b>cts sxp retry period</b>, <b>cts sxp reconcile period</b>, <b>cts sxp connection peer</b>, <b>cts import-pac</b>, <b>cts refresh environment-data</b>, <b>object-group security</b>, <b>security-group</b>, <b>show running-config cts</b>, <b>show running-config object-group</b>, <b>clear configure cts</b>, <b>clear configure object-group</b>, <b>show cts</b>, <b>show object-group</b>, <b>show conn security-group</b>, <b>clear cts</b>, <b>debug cts</b>.</p> <p>We introduced the following MIB: CISCO-TRUSTSEC-SXP-MIB.</p> <p>We introduced or modified the following screens:</p> <p>Configuration &gt; Firewall &gt; Identity by TrustSec  Configuration &gt; Firewall &gt; Objects &gt; Security Groups Object Groups  Configuration &gt; Firewall &gt; Access Rules &gt; Add Access Rules  Monitoring &gt; Properties &gt; Identity by TrustSec &gt; PAC  Monitoring &gt; Properties &gt; Identity by TrustSec &gt; Environment Data  Monitoring &gt; Properties &gt; Identity by TrustSec &gt; SXP Connections  Monitoring &gt; Properties &gt; Identity by TrustSec &gt; IP Mappings  Monitoring &gt; Properties &gt; Connections  Tools &gt; Packet Tracer</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Cisco Cloud Web Security (ScanSafe)	<p>Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity.</p> <p><b>Note</b>    Clientless SSL VPN is not supported with Cloud Web Security; be sure to exempt any clientless SSL VPN traffic from the ASA service policy for Cloud Web Security.</p> <p>We introduced or modified the following commands: <b>class-map type inspect scansafe</b>, <b>default user group</b>, <b>http[s]</b> (parameters), <b>inspect scansafe</b>, <b>license</b>, <b>match user group</b>, <b>policy-map type inspect scansafe</b>, <b>retry-count</b>, <b>scansafe</b>, <b>scansafe general-options</b>, <b>server {primary   backup}</b>, <b>show conn scansafe</b>, <b>show scansafe server</b>, <b>show scansafe statistics</b>, <b>user-identity monitor</b>, <b>whitelist</b>.</p> <p>We introduced or modified the following screens:</p> <p>Configuration &gt; Device Management &gt; Cloud Web Security  Configuration &gt; Firewall &gt; Objects &gt; Class Maps &gt; Cloud Web Security  Configuration &gt; Firewall &gt; Objects &gt; Class Maps &gt; Cloud Web Security &gt; Add/Edit  Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; Cloud Web Security  Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; Cloud Web Security &gt; Add/Edit  Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; Cloud Web Security &gt; Add/Edit &gt; Manage Cloud Web Security Class Maps  Configuration &gt; Firewall &gt; Identity Options  Configuration &gt; Firewall &gt; Service Policy Rules  Monitoring &gt; Properties &gt; Cloud Web Security</p>
Extended ACL and object enhancement to filter ICMP traffic by ICMP code	<p>ICMP traffic can now be permitted/denied based on ICMP code.</p> <p>We introduced or modified the following commands: <b>access-list extended</b>, <b>service-object</b>, <b>service</b>.</p> <p>We introduced or modified the following screens:</p> <p>Configuration &gt; Firewall &gt; Objects &gt; Service Objects/Groups  Configuration &gt; Firewall &gt; Access Rule</p>
Unified communications support on the ASASM	The ASASM now supports all Unified Communications features.
NAT support for reverse DNS lookups	NAT now supports translation of the DNS PTR record for reverse DNS lookups when using IPv4 NAT, IPv6 NAT, and NAT64 with DNS inspection enabled for the NAT rule.



**Table 7**      **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)**

Feature	Description
Per-session PAT	<p>The per-session PAT feature improves the scalability of PAT and, for ASA clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For “hit-and-run” traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address. Without the per-session feature, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With the per-session feature, the connection rate for one address for an IP protocol is 65535/average-lifetime.</p> <p>By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. For traffic that can benefit from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT by creating a per-session deny rule.</p> <p>We introduced the following commands: <b>xlate per-session</b>, <b>clear configure xlate</b>, <b>show running-config xlate</b>.</p> <p>We introduced the following screen: Configuration &gt; Firewall &gt; Advanced &gt; Per-Session NAT Rules.</p>
ARP cache additions for non-connected subnets	<p>The ASA ARP cache only contains entries from directly-connected subnets by default. You can now enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.</p> <p>You may want to use this feature if you use:</p> <ul style="list-style-type: none"> <li>• Secondary subnets.</li> <li>• Proxy ARP on adjacent routes for traffic forwarding.</li> </ul> <p>We introduced the following command: <b>arp permit-nonconnected</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Advanced &gt; ARP &gt; ARP Static Table.</p> <p><i>Also available in 8.4(5).</i></p>
SunRPC change from dynamic ACL to pin-hole mechanism	<p>Previously, Sun RPC inspection does not support outbound access lists because the inspection engine uses dynamic access lists instead of secondary connections.</p> <p>In this release, when you configure dynamic access lists on the ASA, they are supported on the ingress direction only and the ASA drops egress traffic destined to dynamic ports. Therefore, Sun RPC inspection implements a pinhole mechanism to support egress traffic. Sun RPC inspection uses this pinhole mechanism to support outbound dynamic access lists.</p> <p><i>Also available in 8.4(4.1).</i></p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Inspection reset action change	<p>Previously, when the ASA dropped a packet due to an inspection engine rule, the ASA sent only one RST to the source device of the dropped packet. This behavior could cause resource issues.</p> <p>In this release, when you configure an inspection engine to use a reset action and a packet triggers a reset, the ASA sends a TCP reset under the following conditions:</p> <ul style="list-style-type: none"> <li>• The ASA sends a TCP reset to the inside host when the <b>service resetoutbound</b> command is enabled. (The <b>service resetoutbound</b> command is disabled by default.)</li> <li>• The ASA sends a TCP reset to the outside host when the <b>service resetinbound</b> command is enabled. (The <b>service resetinbound</b> command is disabled by default.)</li> </ul> <p>For more information, see the <b>service</b> command in the ASA <i>Cisco ASA 5500 Series Command Reference</i>.</p> <p>This behavior ensures that a reset action will reset the connections on the ASA and on inside servers; therefore countering denial of service attacks. For outside hosts, the ASA does not send a reset by default and information is not revealed through a TCP reset.</p> <p><i>Also available in 8.4(4.1).</i></p>
Increased maximum connection limits for service policy rules	<p>The maximum number of connections for service policy rules was increased from 65535 to 2000000.</p> <p>We modified the following commands: <b>set connection conn-max</b>, <b>set connection embryonic-conn-max</b>, <b>set connection per-client-embryonic-max</b>, <b>set connection per-client-max</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Connection Settings.</p> <p><i>Also available in 8.4(5)</i></p>
<b>High Availability and Scalability Features</b>	

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
ASA Clustering for the ASA 5580 and 5585-X	<p>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. ASA clustering is supported for the ASA 5580 and the ASA 5585-X; all units in a cluster must be the same model with the same hardware specifications. See the configuration guide for a list of unsupported features when clustering is enabled.</p> <p>We introduced or modified the following commands: <b>channel-group</b>, <b>clacp system-mac</b>, <b>clear cluster info</b>, <b>clear configure cluster</b>, <b>cluster exec</b>, <b>cluster group</b>, <b>cluster interface-mode</b>, <b>cluster-interface</b>, <b>conn-rebalance</b>, <b>console-replicate</b>, <b>cluster master unit</b>, <b>cluster remove unit</b>, <b>debug cluster</b>, <b>debug lacp cluster</b>, <b>enable</b> (cluster group), <b>health-check</b>, <b>ip address</b>, <b>ipv6 address</b>, <b>key</b> (cluster group), <b>local-unit</b>, <b>mac-address</b> (interface), <b>mac-address pool</b>, <b>mtu cluster</b>, <b>port-channel span-cluster</b>, <b>priority</b> (cluster group), <b>prompt cluster-unit</b>, <b>show asp cluster counter</b>, <b>show asp table cluster chash-table</b>, <b>show cluster</b>, <b>show cluster info</b>, <b>show cluster user-identity</b>, <b>show lacp cluster</b>, <b>show running-config cluster</b>.</p> <p>We introduced or modified the following screens:</p> <p>Home &gt; Device Dashboard  Home &gt; Cluster Dashboard  Home &gt; Cluster Firewall Dashboard  Configuration &gt; Device Management &gt; Advanced &gt; Address Pools &gt; MAC Address Pools  Configuration &gt; Device Management &gt; High Availability and Scalability &gt; ASA Cluster  Configuration &gt; Device Management &gt; Logging &gt; Syslog Setup &gt; Advanced  Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface &gt; Advanced  Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface &gt; IPv6  Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit EtherChannel Interface &gt; Advanced  Configuration &gt; Firewall &gt; Advanced &gt; Per-Session NAT Rules  Monitoring &gt; ASA Cluster  Monitoring &gt; Properties &gt; System Resources Graphs &gt; Cluster Control Link  Tools &gt; Preferences &gt; General  Tools &gt; System Reload  Tools &gt; Upgrade Software from Local Computer  Wizards &gt; High Availability and Scalability Wizard  Wizards &gt; Packet Capture Wizard  Wizards &gt; Startup Wizard</p>
OSPF, EIGRP, and Multicast for clustering	<p>For OSPFv2 and OSPFv3, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment.</p> <p>For EIGRP, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment.</p> <p>Multicast routing supports clustering.</p> <p>We introduced or modified the following commands: <b>show route cluster</b>, <b>debug route cluster</b>, <b>show mfib cluster</b>, <b>debug mfib cluster</b>.</p>

Table 7 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Packet capture for clustering	<p>To support cluster-wide troubleshooting, you can enable capture of cluster-specific traffic on the master unit using the <b>cluster exec capture</b> command, which is then automatically enabled on all of the slave units in the cluster. The <b>cluster exec</b> keywords are the new keywords that you place in front of the <b>capture</b> command to enable cluster-wide capture.</p> <p>We modified the following commands: <b>capture</b>, <b>show capture</b>.</p> <p>We modified the following screen: Wizards &gt; Packet Capture Wizard.</p>
Logging for clustering	<p>Each unit in the cluster generates syslog messages independently. You can use the <b>logging device-id</b> command to generate syslog messages with identical or different device IDs to make messages appear to come from the same or different units in the cluster.</p> <p>We modified the following command: <b>logging device-id</b>.</p> <p>We modified the following screen: Configuration &gt; Logging &gt; Syslog Setup &gt; Advanced &gt; Advanced Syslog Configuration.</p>
Configure the connection replication rate during a bulk sync	<p>You can now configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASA is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synchronized.</p> <p>We introduced the following command: <b>failover replication rate rate</b>.</p> <p><i>Also available in 8.4(4.1) and 8.5(1.7).</i></p>
<b>IPv6 Features</b>	
IPv6 Support on the ASA's outside interface for VPN Features.	<p>This release of the ASA adds support for IPv6 VPN connections to its outside interface using SSL and IKEv2/IPsec protocols.</p> <p>This release of the ASA continues to support IPv6 VPN traffic on its inside interface using the SSL protocol as it has in the past. This release does not provide IKEv2/IPsec protocol on the inside interface.</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Remote Access VPN support for IPv6: IPv6 Address Assignment Policy	<p>You can configure the ASA to assign an IPv4 address, an IPv6 address, or both an IPv4 and an IPv6 address to an AnyConnect client by creating internal pools of addresses on the ASA or by assigning a dedicated address to a local user on the ASA.</p> <p>The endpoint must have the dual-stack protocol implemented in its operating system to be assigned both types of addresses.</p> <p>Assigning an IPv6 address to the client is supported for the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We introduced the following commands: <b>ipv6-vpn-addr-assign</b>, <b>vpn-framed-ipv6-address</b>.</p> <p>We modified the following screens:</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Address Assignment &gt; Assignment Policy</p> <p>Configuration &gt; Remote Access VPN &gt; AAA/Local Users &gt; Local Users &gt; (Edit local user account) &gt; VPN Policy</p>
Remote Access VPN support for IPv6: Assigning DNS Servers with IPv6 Addresses to group policies	<p>DNS servers can be defined in a Network (Client) Access internal group policy on the ASA. You can specify up to four DNS server addresses including up to two IPv4 addresses and up to two IPv6 addresses.</p> <p>DNS servers with IPv6 addresses can be reached by VPN clients when they are configured to use the SSL protocol. This feature is not supported for clients configured to use the IKEv2/IPsec protocol.</p> <p>We modified the following command: <b>dns-server value</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; (Edit group policy) &gt; Servers.</p>
Remote Access VPN support for IPv6: Split tunneling	<p>Split tunneling enables you to route some network traffic through the VPN tunnel (encrypted) and to route other network traffic outside the VPN tunnel (unencrypted or “in the clear”). You can now perform split tunneling on IPv6 network traffic by defining an IPv6 policy which specifies a unified access control rule.</p> <p>IPv6 split tunneling is reported with the telemetric data sent by the Smart Call Home feature. If either IPv4 or IPv6 split tunneling is enabled, Smart Call Home reports split tunneling as “enabled.” For telemetric data, the VPN session database displays the IPv6 data typically reported with session management.</p> <p>You can include or exclude IPv6 traffic from the VPN “tunnel” for VPN clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We introduced the following command: <b>ipv6-split-tunnel-policy</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; (Edit group policy) &gt; Advanced &gt; Split Tunneling.</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Remote Access VPN support for IPv6: AnyConnect Client Firewall Rules	<p>Access control rules for client firewalls support access list entries for both IPv4 and IPv6 addresses.</p> <p>ACLs containing IPv6 addresses can be applied to clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We modified the following command: <b>anyconnect firewall-rule</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; (Edit group policy) &gt; Advanced &gt; AnyConnect Client &gt; Client Firewall.</p>
Remote Access VPN support for IPv6: Client Protocol Bypass	<p>The Client Protocol Bypass feature allows you to configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.</p> <p>When the AnyConnect client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or “in the clear.”</p> <p>For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.</p> <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We introduced the following command: <b>client-bypass-protocol</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; (Group Policy) Advanced &gt; AnyConnect Client &gt; Client Bypass Protocol.</p>
Remote Access VPN support for IPv6: IPv6 Interface ID and prefix	<p>You can now specify a dedicated IPv6 address for local VPN users.</p> <p>This feature benefits users configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We introduced the following command: <b>vpn-framed-ipv6-address</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; AAA/Local Users &gt; Local Users &gt; (Edit User) &gt; VPN Policy.</p>
Remote Access VPN support for IPv6: Sending ASA FQDN to AnyConnect client	<p>You can return the FQDN of the ASA to the AnyConnect client to facilitate load balancing and session roaming.</p> <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We introduced the following command: <b>gateway-fqdn</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; (Edit group policy) &gt; Advanced &gt; AnyConnect.</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Remote Access VPN support for IPv6: ASA VPN Load Balancing	<p>Clients with IPv6 addresses can make AnyConnect connections through the public-facing IPv6 address of the ASA cluster or through a GSS server. Likewise, clients with IPv6 addresses can make AnyConnect VPN connections through the public-facing IPv4 address of the ASA cluster or through a GSS server. Either type of connection can be load-balanced within the ASA cluster.</p> <p>For clients with IPv6 addresses to successfully connect to the ASAs public-facing IPv4 address, a device that can perform network address translation from IPv6 to IPv4 needs to be in the network.</p> <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We modified the following commands: <b>show run vpn load-balancing</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Load Balancing.</p>
Remote Access VPN support for IPv6: Dynamic Access Policies support IPv6 attributes	<p>When using ASA 9.0 or later with ASDM 6.8 or later, you can now specify these attributes as part of a dynamic access policy (DAP):</p> <ul style="list-style-type: none"> <li>• IPv6 addresses as a Cisco AAA attribute</li> <li>• IPv6 TCP and UDP ports as part of a Device endpoint attribute</li> <li>• Network ACL Filters (client)</li> </ul> <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We modified the following screens:</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Dynamic Access Policies &gt; Add &gt; Cisco AAA attribute</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Dynamic Access Policies &gt; Add &gt; Device &gt; Add Endpoint Attribute</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Dynamic Access Policies &gt; Network ACL Filters (client)</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Dynamic Access Policies &gt; Webtype ACL Filters (clientless)</p>
Remote Access VPN support for IPv6: Session Management	<p>Session management output displays the IPv6 addresses in Public/Assigned address fields for AnyConnect connections, site-to-site VPN connections, and Clientless SSL VPN connections. You can add new filter keywords to support filtering the output to show only IPv6 (outside or inside) connections. No changes to IPv6 User Filters exist.</p> <p>This feature can be used by clients configured to use the SSL protocol. This feature does not support IKEv2/IPsec protocol.</p> <p>We modified the following command: <b>show vpn-sessiondb</b>.</p> <p>We modified these screen: Monitoring &gt; VPN &gt; VPN Statistics &gt; Sessions.</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
NAT support for IPv6	<p>NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6 (NAT64). Translating between IPv4 and IPv6 is not supported in transparent mode.</p> <p>We modified the following commands: <b>nat</b> (in global and object network configuration mode), <b>show conn</b>, <b>show nat</b>, <b>show nat pool</b>, <b>show xlate</b>.</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; Objects &gt; Network Objects/Group  Configuration &gt; Firewall &gt; NAT Rules</p>
DHCPv6 relay	<p>DHCP relay is supported for IPv6.</p> <p>We introduced the following commands: <b>ipv6 dhcprelay server</b>, <b>ipv6 dhcprelay enable</b>, <b>ipv6 dhcprelay timeout</b>, <b>clear config ipv6 dhcprelay</b>, <b>ipv6 nd managed-config-flag</b>, <b>ipv6 nd other-config-flag</b>, <b>debug ipv6 dhcp</b>, <b>debug ipv6 dhcprelay</b>, <b>show ipv6 dhcprelay binding</b>, <b>clear ipv6 dhcprelay binding</b>, <b>show ipv6 dhcprelay statistics</b>, and <b>clear ipv6 dhcprelay statistics</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Relay.</p>



**Table 7**      **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)**

Feature	Description
OSPFv3	<p>OSPFv3 routing is supported for IPv6. Note the following additional guidelines and limitations for OSPFv2 and OSPFv3:</p> <p><b>Clustering</b></p> <ul style="list-style-type: none"> <li>• OSPFv2 and OSPFv3 support clustering.</li> <li>• When clustering is configured, OSPFv3 encryption is not supported. An error message appears if you try to configure OSPFv3 encryption in a clustering environment.</li> <li>• When using individual interfaces, make sure that you establish the master and slave units as either OSPFv2 or OSPFv3 neighbors.</li> <li>• When using individual interfaces, OSPFv2 adjacencies can only be established between two contexts on a shared interface on the master unit. Configuring static neighbors is supported only on point-to-point links; therefore, only one neighbor statement is allowed on an interface.</li> </ul> <p><b>Other</b></p> <ul style="list-style-type: none"> <li>• OSPFv2 and OSPFv3 support multiple instances on an interface.</li> <li>• The ESP and AH protocol is supported for OSPFv3 authentication.</li> <li>• OSPFv3 supports Non-Payload Encryption.</li> </ul> <p>We introduced or modified the following commands: <b>ipv6 ospf cost</b>, <b>ipv6 ospf database-filter all out</b>, <b>ipv6 ospf dead-interval</b>, <b>ipv6 ospf hello-interval</b>, <b>ipv6 ospf mtu-ignore</b>, <b>ipv6 ospf neighbor</b>, <b>ipv6 ospf network</b>, <b>ipv6 ospf priority</b>, <b>ipv6 ospf retransmit-interval</b>, <b>ipv6 ospf transmit-delay</b>, <b>ipv6 router ospf</b>, <b>ipv6 router ospf area</b>, <b>ipv6 router ospf default</b>, <b>ipv6 router ospf default-information</b>, <b>ipv6 router ospf distance</b>, <b>ipv6 router ospf exit</b>, <b>ipv6 router ospf ignore</b>, <b>ipv6 router ospf log-adjacency-changes</b>, <b>ipv6 router ospf no</b>, <b>ipv6 router ospf redistribute</b>, <b>ipv6 router ospf router-id</b>, <b>ipv6 router ospf summary-prefix</b>, <b>ipv6 router ospf timers</b>, <b>area range</b>, <b>area virtual-link</b>, <b>default</b>, <b>default-information originate</b>, <b>distance</b>, <b>ignore lsa mospf</b>, <b>log-adjacency-changes</b>, <b>redistribute</b>, <b>router-id</b>, <b>summary-prefix</b>, <b>timers lsa arrival</b>, <b>timers pacing flood</b>, <b>timers pacing lsa-group</b>, <b>timers pacing retransmission</b>, <b>show ipv6 ospf</b>, <b>show ipv6 ospf border-routers</b>, <b>show ipv6 ospf database-filter</b>, <b>show ipv6 ospf flood-list</b>, <b>show ipv6 ospf interface</b>, <b>show ipv6 ospf neighbor</b>, <b>show ipv6 ospf request-list</b>, <b>show ipv6 ospf retransmission-list</b>, <b>show ipv6 ospf summary-prefix</b>, <b>show ipv6 ospf virtual-links</b>, <b>show ospf</b>, <b>show run ipv6 router</b>, <b>clear ipv6 ospf</b>, <b>clear configure ipv6 router</b>, <b>debug ospfv3</b>.</p> <p>We introduced the following screens:</p> <p>Configuration &gt; Device Setup &gt; Routing &gt; OSPFv3 &gt; Setup  Configuration &gt; Device Setup &gt; Routing &gt; OSPFv3 &gt; Interface  Configuration &gt; Device Setup &gt; Routing &gt; OSPFv3 &gt; Redistribution  Configuration &gt; Device Setup &gt; Routing &gt; OSPFv3 &gt; Summary Prefix  Configuration &gt; Device Setup &gt; Routing &gt; OSPFv3 &gt; Virtual Link  Monitoring &gt; Routing &gt; OSPFv3 LSAs  Monitoring &gt; Routing &gt; OSPFv3 Neighbors</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Unified ACL for IPv4 and IPv6	<p>ACLs now support IPv4 and IPv6 addresses. You can also specify a mix of IPv4 and IPv6 addresses for the source and destination. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs.</p> <p>ACLs containing IPv6 addresses can be applied to clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We modified the following commands: <b>access-list extended</b>, <b>access-list webtype</b>.</p> <p>We removed the following commands: <b>ipv6 access-list</b>, <b>ipv6 access-list webtype</b>, <b>ipv6-vpn-filter</b>.</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; Access Rules  Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; General &gt; More Options</p>
Mixed IPv4 and IPv6 object groups	<p>Previously, network object groups could only contain all IPv4 addresses or all IPv6 addresses. Now network object groups can support a mix of both IPv4 and IPv6 addresses.</p> <p><b>Note</b> You cannot use a mixed object group for NAT.</p> <p>We modified the following command: <b>object-group network</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Objects &gt; Network Objects/Groups.</p>
Range of IPv6 addresses for a Network object	<p>You can now configure a range of IPv6 addresses for a network object.</p> <p>We modified the following command: <b>range</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Objects &gt; Network Objects/Groups.</p>
Inspection support for IPv6 and NAT64	<p>We now support DNS inspection for IPv6 traffic.</p> <p>We also support translating between IPv4 and IPv6 for the following inspections:</p> <ul style="list-style-type: none"> <li>• DNS</li> <li>• FTP</li> <li>• HTTP</li> <li>• ICMP</li> </ul> <p>You can now also configure the service policy to generate a syslog message (767001) when unsupported inspections receive and drop IPv6 traffic.</p> <p>We modified the following command: <b>service-policy fail-close</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard - Service Policy.</p>

**Remote Access Features**

**Table 7**      **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)**

Feature	Description
Clientless SSL VPN: Additional Support	<p>We have added additional support for these browsers, operating systems, web technologies and applications:</p> <p><b>Internet browser support:</b> Microsoft Internet Explorer 9, Firefox 4, 5, 6, 7, and 8</p> <p><b>Operating system support:</b> Mac OS X 10.7</p> <p><b>Web technology support:</b> HTML 5</p> <p><b>Application Support:</b> Sharepoint 2010</p>
Clientless SSL VPN: Enhanced quality for rewriter engines	<p>The clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN users.</p> <p>We did not add or modify any commands for this feature.</p> <p>We did not add or modify any ASDM screens for this feature.</p> <p><i>Also available in 8.4(4.1).</i></p>
Clientless SSL VPN: Citrix Mobile Receiver	<p>This feature provides secure remote access for Citrix Receiver applications running on mobile devices to XenApp and XenDesktop VDI servers through the ASA.</p> <p>For the ASA to proxy Citrix Receiver to a Citrix Server, when users try to connect to Citrix virtualized resource, instead of providing the Citrix Server's address and credentials, users enter the ASA's SSL VPN IP address and credentials.</p> <p>We modified the following command: <b>vdci</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Group Policy &gt; Edit &gt; More Options &gt; VDI Access &gt; Add VDI Server.</p>
Clientless SSL VPN: Enhanced Auto-sign-on	<p>This feature improves support for web applications that require dynamic parameters for authentication.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Bookmarks.</p>
Clientless SSL VPN: Clientless Java Rewriter Proxy Support	<p>This feature provides proxy support for clientless Java plug-ins when a proxy is configured in client machines' browsers.</p> <p>We did not add or modify any commands for this feature.</p> <p>We did not add or modify any ASDM screens for this feature.</p>
Clientless SSL VPN: Remote File Explorer	<p>The Remote File Explorer provides users with a way to browse the corporate network from their web browser. When users click the Remote File System icon on the Cisco SSL VPN portal page, an applet is launched on the user's system displaying the remote file system in a tree and folder view.</p> <p>We did not add or modify any commands for this feature.</p> <p>We did not add or modify any ASDM screens for this feature.</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Clientless SSL VPN: Server Certificate Validation	<p>This feature enhances clientless SSL VPN support to enable SSL server certificate verification for remote HTTPS sites against a list of trusted CA certificates.</p> <p>We modified the following commands: <b>ssl-server-check</b>, <b>crypto</b>, <b>crypto ca trustpool</b>, <b>crl</b>, <b>certificate</b>, <b>revocation-check</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Certificate Management &gt; Trusted Certificate Pool.</p>
AnyConnect Performance Improvements	<p>This feature improves throughput performance for AnyConnect TLS/DTLS traffic in multi-core platforms. It accelerates the SSL VPN datapath and provides customer-visible performance gains in AnyConnect, smart tunnels, and port forwarding.</p> <p>We modified the following commands: <b>crypto engine accelerator-bias</b> and <b>show crypto accelerator</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Advanced &gt; Crypto Engine.</p>
Custom Attributes	<p>Custom attributes define and configure AnyConnect features that have not yet been added to ASDM. You add custom attributes to a group policy, and define values for those attributes.</p> <p>For AnyConnect 3.1, custom attributes are available to support AnyConnect Deferred Upgrade.</p> <p>Custom attributes can benefit AnyConnect clients configured for either IKEv2/IPsec or SSL protocols.</p> <p>We added the following command: <b>anyconnect-custom-attr</b>.</p> <p>A new screen was added: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; AnyConnect Custom Attributes.</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Next Generation Encryption	<p>The National Standards Association (NSA) specified a set of cryptographic algorithms that devices must support to meet U.S. federal standards for cryptographic strength. RFC 6379 defines the Suite B cryptographic suites. Because the collective set of algorithms defined as NSA Suite B are becoming a standard, the AnyConnect IPsec VPN (IKEv2 only) and public key infrastructure (PKI) subsystems now support them. The next generation encryption (NGE) includes a larger superset of this set adding cryptographic algorithms for IPsec V3 VPN, Diffie-Hellman Groups 14 and 24 for IKEv2, and RSA certificates with 4096 bit keys for DTLS and IKEv2.</p> <p>The following functionality is added to ASA to support the Suite B algorithms:</p> <ul style="list-style-type: none"> <li>• AES-GCM/GMAC support (128-, 192-, and 256-bit keys) <ul style="list-style-type: none"> <li>– IKEv2 payload encryption and authentication</li> <li>– ESP packet encryption and authentication</li> <li>– Hardware supported only on multi-core platforms</li> </ul> </li> <li>• SHA-2 support (256-, 384-, and 512-bit hashes) <ul style="list-style-type: none"> <li>– ESP packet authentication</li> <li>– Hardware and software supported only on multi-core platforms</li> </ul> </li> <li>• ECDH support (groups 19, 20, and 21) <ul style="list-style-type: none"> <li>– IKEv2 key exchange</li> <li>– IKEv2 PFS</li> <li>– Software only supported on single- or multi-core platforms</li> </ul> </li> <li>• ECDSA support (256-, 384-, and 521-bit elliptic curves) <ul style="list-style-type: none"> <li>– IKEv2 user authentication</li> <li>– PKI certificate enrollment</li> <li>– PKI certificate generation and verification</li> <li>– Software only supported on single- or multi-core platforms</li> </ul> </li> </ul> <p>New cryptographic algorithms are added for IPsecV3.</p> <p><b>Note</b> Suite B algorithm support requires an AnyConnect Premium license for IKEv2 remote access connections, but Suite B usage for other connections or purposes (such as PKI) has no limitations. IPsecV3 has no licensing restrictions.</p> <p>We introduced or modified the following commands: <b>crypto ikev2 policy</b>, <b>crypto ipsec ikev2 ipsec-proposal</b>, <b>crypto key generate</b>, <b>crypto key zeroize</b>, <b>show crypto key mypubkey</b>, <b>show vpn-sessiondb</b>.</p> <p>We introduced or modified the following screens:</p> <p>Monitor &gt; VPN &gt; Sessions  Monitor &gt; VPN &gt; Encryption Statistics  Configuration &gt; Site-to-Site VPN &gt; Certificate Management &gt; Identity Certificates  Configuration &gt; Site-to-Site VPN &gt; Advanced &gt; System Options  Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; IPsec &gt; Crypto Maps</p>

**Table 7**      ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Support for VPN on the ASASM	The ASASM now supports all VPN features.
<b>Multiple Context Mode Features</b>	
Site-to-Site VPN in multiple context mode	Site-to-site VPN tunnels are now supported in multiple context mode.
New resource type for site-to-site VPN tunnels	<p>New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.</p> <p>We modified the following commands: <b>limit-resource</b>, <b>show resource types</b>, <b>show resource usage</b>, <b>show resource allocation</b>.</p> <p>We modified the following screen: Configuration &gt; Context Management &gt; Resource Class &gt; Add Resource Class.</p>
Dynamic routing in Security Contexts	EIGRP and OSPFv2 dynamic routing protocols are now supported in multiple context mode. OSPFv3, RIP, and multicast routing are not supported.
New resource type for routing table entries	<p>A new resource class, routes, was created to set the maximum number of routing table entries in each context.</p> <p>We modified the following commands: <b>limit-resource</b>, <b>show resource types</b>, <b>show resource usage</b>, <b>show resource allocation</b>.</p> <p>We modified the following screen: Configuration &gt; Context Management &gt; Resource Class &gt; Add Resource Class.</p>
Mixed firewall mode support in multiple context mode	<p>You can set the firewall mode independently for each security context in multiple context mode, so some can run in transparent mode while others run in routed mode.</p> <p>We modified the following command: <b>firewall transparent</b>.</p> <p>You cannot set the firewall mode in ASDM; you must use the command-line interface.</p> <p><i>Also available in Version 8.5(1).</i></p>
<b>Module Features</b>	
ASA Services Module support on the Cisco 7600 switch	<p>The Cisco 7600 series now supports the ASASM. For specific hardware and software requirements, see:</p> <p><a href="http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html">http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html</a>.</p>

**Table 7**      **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)**

Feature	Description
ASA 5585-X support for the ASA CX SSP-10 and -20	<p>The ASA CX module lets you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees.</p> <p>We introduced or modified the following commands: <b>capture</b>, <b>cxsc</b>, <b>cxsc auth-proxy</b>, <b>debug cxsc</b>, <b>hw-module module password-reset</b>, <b>hw-module module reload</b>, <b>hw-module module reset</b>, <b>hw-module module shutdown</b>, <b>session do setup host ip</b>, <b>session do get-config</b>, <b>session do password-reset</b>, <b>show asp table classify domain cxsc</b>, <b>show asp table classify domain cxsc-auth-proxy</b>, <b>show capture</b>, <b>show conn</b>, <b>show module</b>, <b>show service-policy</b>.</p> <p>We introduced the following screens:</p> <p>Home &gt; ASA CX Status  Wizards &gt; Startup Wizard &gt; ASA CX Basic Configuration  Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule &gt; Rule Actions &gt; ASA CX Inspection</p> <p><i>Also available in 8.4(4.1).</i></p>
ASA 5585-X Dual SSP support for the SSP-10 and SSP-20 (in addition to the SSP-40 and SSP-60); VPN support for Dual SSPs	<p>The ASA 5585-X now supports dual SSPs using all SSP models (you can use two SSPs of the same level in the same chassis). VPN is now supported when using dual SSPs.</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p>

## New Features in Version 8.7

This section includes the following topics:

- [New Features in ASA 8.7\(1.1\)/ASDM 6.7\(1\), page 31](#)

## New Features in ASA 8.7(1.1)/ASDM 6.7(1)

**Released: October 16, 2012**

**Table 8** lists the new features for ASA Version 8.7(1.1)/ASDM Version 6.7(1).



### Note

Version 8.7(1) was removed from Cisco.com due to build issues; please upgrade to Version 8.7(1.1) or later.

**Table 8**      ***New Features for ASA Version 8.7(1.1)/ASDM Version 6.7(1)***

<b>Feature</b>	<b>Description</b>
<b>Platform Features</b>	
Support for the ASA 1000V	We introduced support for the ASA 1000V for the Nexus 1000V switch.
Cloning the ASA 1000V	You can add one or multiple instances of the ASA 1000V to your deployment using the method of cloning VMs.
<b>Management Features</b>	
ASDM mode	You can configure, manage, and monitor the ASA 1000V using the Adaptive Security Device Manager (ASDM), which is the single GUI-based device manager for the ASA.
VNMC mode	You can configure and manage the ASA 1000V using the Cisco Virtual Network Management Center (VNMC), which is a GUI-based multi-device manager for multiple tenants.
XML APIs	You can configure and manage the ASA 1000V using XML APIs, which are application programmatic interfaces provided through the Cisco VNMC. This feature is only available in VNMC mode.
<b>Firewall Features</b>	
Cisco VNMC access and configuration	Cisco VNMC access and configuration are required to create security profiles. You can configure access to the Cisco VNMC through the Configuration > Device Setup > Interfaces pane in ASDM. Enter the login username and password, hostname, and shared secret to access the Cisco VNMC. Then you can configure security profiles and security profile interfaces. In VNMC mode, use the CLI to configure security profiles.
Security profiles and security profile interfaces	<p>Security profiles are interfaces that correspond to an edge security profile that has been configured in the Cisco VNMC and assigned in the Cisco Nexus 1000V VSM. Policies for through-traffic are assigned to these interfaces and the outside interface. You can add security profiles through the Configuration &gt; Device Setup &gt; Interfaces pane. You create the security profile by adding its name and selecting the service interface. ASDM then generates the security profile through the Cisco VNMC, assigns the security profile ID, and automatically generates a unique interface name. The interface name is used in the security policy configuration.</p> <p>We introduced or modified the following commands: <b>interface security-profile</b>, <b>security-profile</b>, <b>mtu</b>, <b>vpath path-mtu</b>, <b>clear interface security-profile</b>, <b>clear configure interface security-profile</b>, <b>show interface security-profile</b>, <b>show running-config interface security-profile</b>, <b>show interface ip brief</b>, <b>show running-config mtu</b>, <b>show vsn ip binding</b>, <b>show vsn security-profile</b>.</p> <p>We introduced or modified the following screens:</p> <p>Configuration &gt; Device Setup &gt; Interfaces  Configuration &gt; Device Setup &gt; Interfaces &gt; Add Security Profile  Monitoring &gt; Interfaces &gt; Security Profiles</p>



**Table 8**      ***New Features for ASA Version 8.7(1.1)/ASDM Version 6.7(1) (continued)***

Feature	Description
Service interface	<p>The service interface is the Ethernet interface associated with security profile interfaces. You can only configure one service interface, which must be the inside interface.</p> <p>We introduced the following command: <b>service-interface security-profile all</b>.</p> <p>We modified the following screen: Configuration &gt; Device Setup &gt; Interfaces.</p>
VNMC policy agent	<p>The VNMC policy agent enables policy configuration through both the ASDM and VNMC modes. It includes a web server that receives XML-based requests from Cisco VNMC over HTTPS and converts it to the ASA 1000V configuration.</p> <p>We introduced the following commands: <b>vnmc policy-agent, login, shared-secret, registration host, vnmc org, show vnmc policy-agent, show running-config vnmc policy-agent, clear configure vnmc policy-agent</b>.</p> <p>We modified the following screen: Configuration &gt; Device Setup &gt; Interfaces.</p>

## New Features in Version 8.6

This section includes the following topics:

- [New Features in ASA 8.6\(1\)/ASDM 6.6\(1\), page 33](#)

## New Features in ASA 8.6(1)/ASDM 6.6(1)

**Released: February 28, 2012**

[Table 12](#) lists the new features for ASA Version 8.6(1)/ASDM Version 6.6(1). This ASA software version is only supported on the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.



### Note

Version 8.6(1) includes all features in 8.4(2), plus the features listed in this table.

Features added in 8.4(3) are not included in 8.6(1) unless they are explicitly listed in this table.

**Table 9**      ***New Features for ASA Version 8.6(1)/ASDM Version 6.6(1)***

Feature	Description
<b>Hardware Features</b>	
Support for the ASA 5512-X through ASA 5555-X	We introduced support for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.
<b>IPS Features</b>	

**Table 9**      **New Features for ASA Version 8.6(1)/ASDM Version 6.6(1) (continued)**

Feature	Description
Support for the IPS SSP for the ASA 5512-X through ASA 5555-X	<p>We introduced support for the IPS SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.</p> <p>We introduced or modified the following commands: <b>session</b>, <b>show module</b>, <b>sw-module</b>.</p> <p>We did not modify any screens.</p>
<b>Remote Access Features</b>	
Clientless SSL VPN browser support	<p>The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4.</p> <p><i>Also available in Version 8.4(3).</i></p>
Compression for DTLS and TLS	<p>To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients.</p> <p><b>Note</b>    Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced.</p> <p>We introduced or modified the following commands: <b>anyconnect dtls compression [lzs   none]</b> and <b>anyconnect ssl compression [deflate   lzs   none]</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Group Policies &gt; Edit &gt; Edit Internal Group Policy &gt; Advanced &gt; AnyConnect Client &gt; SSL Compression.</p> <p><i>Also available in Version 8.4(3).</i></p>
Clientless SSL VPN Session Timeout Alerts	<p>Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout.</p> <p>We introduced the following commands: <b>vpn-session-timeout alert-interval</b>, <b>vpn-idle-timeout alert-interval</b>.</p> <p>We introduced the following screens:</p> <p>Remote Access VPN &gt; Configuration &gt; Clientless SSL VPN Access &gt; Portal &gt; Customizations &gt; Add/Edit &gt; Timeout Alerts</p> <p>Remote Access VPN &gt; Configuration &gt; Clientless SSL VPN Access &gt; Group Policies &gt; Add/Edit General</p> <p><i>Also available in Version 8.4(3).</i></p>
<b>Multiple Context Mode Features</b>	

**Table 9**      **New Features for ASA Version 8.6(1)/ASDM Version 6.6(1) (continued)**

Feature	Description
Automatic generation of a MAC address prefix	<p>In multiple context mode, the ASA now converts the automatic MAC address generation configuration to use a default prefix. The ASA auto-generates the prefix based on the last two bytes of the interface MAC address. This conversion happens automatically when you reload, or if you reenables MAC address generation. The prefix method of generation provides many benefits, including a better guarantee of unique MAC addresses on a segment. You can view the auto-generated prefix by entering the <b>show running-config mac-address</b> command. If you want to change the prefix, you can reconfigure the feature with a custom prefix. The legacy method of MAC address generation is no longer available.</p> <p><b>Note</b> To maintain hitless upgrade for failover pairs, the ASA does <i>not</i> convert the MAC address method in an existing configuration upon a reload if failover is enabled. However, we strongly recommend that you manually change to the prefix method of generation. After upgrading, to use the prefix method of MAC address generation, reenables MAC address generation to use the default prefix.</p> <p>We modified the following command: <b>mac-address auto</b>.</p> <p>We modified the following screen: Configuration &gt; Context Management &gt; Security Contexts</p>
<b>AAA Features</b>	
Increased maximum LDAP values per attribute	<p>The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037.</p> <p>We introduced the following command: <b>ldap-max-value-range</b> <i>number</i> (Enter this command in aaa-server host configuration mode).</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p> <p><i>Also available in Version 8.4(3).</i></p>
Support for sub-range of LDAP search results	<p>When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.</p> <p><i>Also available in Version 8.4(3).</i></p>
<b>Troubleshooting Features</b>	
Regular expression matching for the <b>show asp table classifier</b> and <b>show asp table filter</b> commands	<p>You can now enter the <b>show asp table classifier</b> and <b>show asp table filter</b> commands with a regular expression to filter output.</p> <p>We modified the following commands: <b>show asp table classifier match</b> <i>regex</i>, <b>show asp table filter match</b> <i>regex</i>.</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p> <p><i>Also available in Version 8.4(3).</i></p>

## New Features in Version 8.5

This section includes the following topics:

- [New Features in ASA 8.5\(1.7\)/ASDM 6.5\(1.101\), page 36](#)
- [New Features in ASA 8.5\(1.6\)/ASDM 6.5\(1\), page 37](#)
- [New Features in ASA 8.5\(1\)/ASDM 6.5\(1\), page 38](#)

## New Features in ASA 8.5(1.7)/ASDM 6.5(1.101)

**Released: March 5, 2012**

[Table 18](#) lists the new features for ASA interim Version 8.5(1.7)/ASDM Version 6.5(1.101).



### Note

We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

**Table 10**      ***New Features for ASA Interim Version 8.5(1.7)/ASDM Version 6.5(1.101)***

Feature	Description
<b>Hardware Features</b>	
Support for the Catalyst 6500 Supervisor 2T	<p>The ASA now interoperates with the Catalyst 6500 Supervisor 2T. For hardware and software compatibility, see: <a href="http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html">http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html</a>.</p> <p><b>Note</b> You may have to upgrade the FPD image on the ASA. See the Upgrading procedure the in the release notes.</p>
<b>Multiple Context Features</b>	
ASDM support for Automatic generation of a MAC address prefix	<p>ASDM now shows that an autogenerated prefix will be used if you do not specify one.</p> <p>We modified the following screen: Configuration &gt; Context Management &gt; Security Contexts</p>

**Table 10**      **New Features for ASA Interim Version 8.5(1.7)/ASDM Version 6.5(1.101) (continued)**

Feature	Description
<b>Failover Features</b>	
Configure the connection replication rate during a bulk sync	<p>You can now configure the rate at which the ASA replicates connections to the standby unit when using stateful failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASA is 8 million; replicating 8 million connections in 15 seconds means creating 533K connections per second. However, the maximum connections allowed per second is 300K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synced.</p> <p>We introduced the following command: <b>failover replication rate</b> <i>rate</i>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; High Availability &gt; Failover.</p>

## New Features in ASA 8.5(1.6)/ASDM 6.5(1)

**Released: January 27, 2012**

[Table 18](#) lists the new features for ASA interim Version 8.5(1.6)/ASDM Version 6.5(1).



### Note

We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

**Table 11**      **New Features for ASA Interim Version 8.5(1.6)/ASDM Version 6.5(1)**

Feature	Description
<b>Multiple Context Features</b>	
Automatic generation of a MAC address prefix	<p>In multiple context mode, the ASA now converts the automatic MAC address generation configuration to use a default prefix. The ASA auto-generates the prefix based on the last two bytes of the backplane MAC address. This conversion happens automatically when you reload, or if you reenables MAC address generation. The prefix method of generation provides many benefits, including a better guarantee of unique MAC addresses on a segment. You can view the auto-generated prefix by entering the <b>show running-config mac-address</b> command. If you want to change the prefix, you can reconfigure the feature with a custom prefix. The legacy method of MAC address generation is no longer available.</p> <p><b>Note</b> To maintain hitless upgrade for failover pairs, the ASA does <i>not</i> convert the MAC address method in an existing configuration upon a reload if failover is enabled. However, we strongly recommend that you manually change to the prefix method of generation when using failover. Without the prefix method, ASASMs installed in different slot numbers experience a MAC address change upon failover, and can experience traffic interruption. After upgrading, to use the prefix method of MAC address generation, reenables MAC address generation to use the default prefix.</p> <p>We modified the following command: <b>mac-address auto</b>.</p> <p>ASDM was not changed.</p>

## New Features in ASA 8.5(1)/ASDM 6.5(1)

**Released: July 8, 2011**

[Table 12](#) lists the new features for ASA Version 8.5(1)/ASDM Version 6.5(1). This ASA and ASDM software version is only supported on the ASASM.



**Note**

Version 8.5(1) includes all features in 8.4(1), plus the features listed in this table. The following features, however, are not supported in No Payload Encryption software, and this release is only available as a No Payload Encryption release:

- VPN
- Unified Communications

Features added in 8.4(2) are not included in 8.5(1) unless they are explicitly listed in this table.

**Table 12**      **New Features for ASA Version 8.5(1)/ASDM Version 6.5(1)**

Feature	Description
<b>Hardware Features</b>	
Support for the ASA Services Module	We introduced support for the ASASM for the Cisco Catalyst 6500 E switch.
<b>Firewall Features</b>	

**Table 12**      **New Features for ASA Version 8.5(1)/ASDM Version 6.5(1) (continued)**

Feature	Description
Mixed firewall mode support in multiple context mode	<p>You can set the firewall mode independently for each security context in multiple context mode, so some can run in transparent mode while others run in routed mode.</p> <p>We modified the following command: <b>firewall transparent</b>.</p> <p>You cannot set the firewall mode in ASDM; you must use the command line interface.</p>
<b>Interface Features</b>	
Automatic MAC address generation is now enabled by default in multiple context mode	<p>Automatic generation of MAC addresses is now enabled by default in multiple context mode.</p> <p>We modified the following command: <b>mac address auto</b>.</p> <p>We modified the following screen: System &gt; Configuration &gt; Context Management &gt; Security Contexts.</p>
<b>NAT Features</b>	
Identity NAT configurable proxy ARP and route lookup	<p>In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was always used to determine the egress interface. You could not configure these settings. In 8.4(2) and later, the default behavior for identity NAT was changed to match the behavior of other static NAT configurations: proxy ARP is enabled, and the NAT configuration determines the egress interface (if specified) by default. You can leave these settings as is, or you can enable or disable them discretely. Note that you can now also disable proxy ARP for regular static NAT.</p> <p>For pre-8.3 configurations, the migration of NAT exempt rules (the <b>nat 0 access-list</b> command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: <b>no-proxy-arp</b> and <b>route-lookup</b>. The <b>unidirectional</b> keyword that was used for migrating to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the <b>no-proxy-arp</b> and <b>route-lookup</b> keywords, to maintain existing functionality. The <b>unidirectional</b> keyword is removed.</p> <p>We modified the following commands: <b>nat static [no-proxy-arp] [route-lookup]</b> (object network) and <b>nat source static [no-proxy-arp] [route-lookup]</b> (global).</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object &gt; Advanced NAT Settings  Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule</p> <p><i>Also available in Version 8.4(2).</i></p>

**Table 12**      ***New Features for ASA Version 8.5(1)/ASDM Version 6.5(1) (continued)***

Feature	Description
PAT pool and round robin address assignment	<p>You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy.</p> <p><b>Note</b>    Currently in 8.5(1), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634).</p> <p>We modified the following commands: <b>nat dynamic</b> [<b>pat-pool</b> mapped_object [<b>round-robin</b>]] (object network) and <b>nat source dynamic</b> [<b>pat-pool</b> mapped_object [<b>round-robin</b>]] (global).</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object  Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule</p> <p><i>Also available in Version 8.4(2).</i></p>
<b>Switch Integration Features</b>	
Autostate	<p>The switch supervisor engine can send autostate messages to the ASASM about the status of physical interfaces associated with ASA VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the ASA that the VLAN is down. This information lets the ASA declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the ASA takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).</p> <p><b>Note</b>    The switch supports autostate messaging only if you install a single ASA in the chassis.</p> <p>See the following Cisco IOS command: <b>firewall autostate</b>.</p>
Virtual Switching System	The ASASM supports VSS when configured on the switches. No ASA configuration is required.

## New Features in Version 8.4

This section includes the following topics:

- [New Features in ASA 8.4\(6\)/ASDM 7.1\(2.102\), page 41](#)
- [New Features in ASA 8.4\(5\)/ASDM 7.0\(2\), page 41](#)
- [New Features in ASA 8.4\(4.5\)/ASDM 6.4\(9.103\), page 43](#)
- [New Features in ASA 8.4\(4.1\)/ASDM 6.4\(9\), page 44](#)
- [New Features in ASA 8.4\(3\)/ASDM 6.4\(7\), page 49](#)
- [New Features in ASA 8.4\(2.8\)/ASDM 6.4\(5.106\), page 52](#)
- [New Features in ASA 8.4\(2\)/ASDM 6.4\(5\), page 54](#)
- [New Features in ASA 8.4\(1.11\)/ASDM 6.4\(2\), page 62](#)



- [New Features in ASA 8.4\(1\)/ASDM 6.4\(1\), page 63](#)

**Note**

Version 8.4(4) and 8.4(4.3) were removed from Cisco.com due to build issues; please upgrade to a later version.

## New Features in ASA 8.4(6)/ASDM 7.1(2.102)

Released: April 29, 2013

[Table 20](#) lists the new features for ASA Version 8.4(6)/ASDM Version 7.1(2.102).

**Table 13**      ***New Features for ASA Version 8.4(6)/ASDM Version 7.1(2.102)***

Feature	Description
<b>Monitoring Features</b>	
Ability to view top 10 memory users	<p>You can now view the top bin sizes allocated and the top 10 PCs for each allocated bin size. Previously, you had to enter multiple commands to see this information (the <b>show memory detail</b> command and the <b>show memory binsize</b> command); the new command provides for quicker analysis of memory issues.</p> <p>We introduced the following command: <b>show memory top-usage</b>.</p> <p>No ASDM changes were made.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>
CPU profile enhancements	<p>The <b>cpu profile activate</b> command now supports the following:</p> <ul style="list-style-type: none"> <li>• Delayed start of the profiler until triggered (global or specific thread CPU %)</li> <li>• Sampling of a single thread</li> </ul> <p>We modified the following command: <b>cpu profile activate</b> [<i>n-samples</i>] [<b>sample-process</b> <i>process-name</i>] [<b>trigger cpu-usage</b> <i>cpu%</i> [<i>process-name</i>]].</p> <p>No ASDM changes were made.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>
<b>Remote Access Features</b>	
<b>user-storage value</b> command password is now encrypted in <b>show</b> commands	<p>The password in the <b>user-storage value</b> command is now encrypted when you enter <b>show running-config</b>.</p> <p>We modified the following command: <b>user-storage value</b>.</p> <p>We modified the following screen: <b>Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Group Policies &gt; More Options &gt; Session Settings</b>.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>

## New Features in ASA 8.4(5)/ASDM 7.0(2)

Released: October 31, 2012

Table 20 lists the new features for ASA Version 8.4(5)/ASDM Version 7.0(2).

**Table 14**      **New Features for ASA Version 8.4(5)/ASDM Version 7.0(2)**

Feature	Description
<b>Firewall Features</b>	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	<p>In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL.</p> <p>We modified the following command: <b>access-list ethertype {permit   deny} is-is</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Management Access &gt; EtherType Rules.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>
ARP cache additions for non-connected subnets	<p>The ASA ARP cache only contains entries from directly-connected subnets by default. You can now enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.</p> <p>You may want to use this feature if you use:</p> <ul style="list-style-type: none"> <li>• Secondary subnets.</li> <li>• Proxy ARP on adjacent routes for traffic forwarding.</li> </ul> <p>We introduced the following command: <b>arp permit-nonconnected</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Advanced &gt; ARP &gt; ARP Static Table.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>
Increased maximum connection limits for service policy rules	<p>The maximum number of connections for service policy rules was increased from 65535 to 2000000.</p> <p>We modified the following commands: <b>set connection conn-max</b>, <b>set connection embryonic-conn-max</b>, <b>set connection per-client-embryonic-max</b>, <b>set connection per-client-max</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Connection Settings.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>
<b>Remote Access Features</b>	
Improved Host Scan and ASA Interoperability	<p>Host Scan and the ASA use an improved process to transfer posture attributes from the client to the ASA. This gives the ASA more time to establish a VPN connection with the client and apply a dynamic access policy.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>
<b>Monitoring Features</b>	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	<p>Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP.</p> <p>This data is equivalent to the <b>show xlate count</b> command.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>

**Table 14**      **New Features for ASA Version 8.4(5)/ASDM Version 7.0(2) (continued)**

Feature	Description
NSEL	<p>Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent.</p> <p>We introduced the following command: <b>flow-export active refresh-interval</b>.</p> <p>We modified the following command: <b>flow-export event-type</b>.</p> <p>We modified the following screens: Configuration &gt; Device Management &gt; Logging &gt; NetFlow.</p> <p>Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard - Rule Actions &gt; NetFlow &gt; Add Flow Event</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>
<b>Hardware Features</b>	
ASA 5585-X DC power supply support	<p>Support was added for the ASA 5585-X DC power supply.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>

## New Features in ASA 8.4(4.5)/ASDM 6.4(9.103)

**Released: August 13, 2012**

[Table 20](#) lists the new features for ASA interim Version 8.4(4.5)/ASDM Version 6.4(9.103).



### Note

Version 8.4(4.3) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.5) or later.



### Note

We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the interim release notes available on the Cisco.com software download site.

**Table 15**      **New Features for ASA Version 8.4(4.5)/ASDM Version 6.4(9.103)**

Feature	Description
<b>Firewall Features</b>	
ARP cache additions for non-connected subnets	<p>The ASA ARP cache only contains entries from directly-connected subnets by default. You can now enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.</p> <p>You may want to use this feature if you use:</p> <ul style="list-style-type: none"> <li>• Secondary subnets.</li> <li>• Proxy ARP on adjacent routes for traffic forwarding.</li> </ul> <p>We introduced the following command: <b>arp permit-nonconnected</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Advanced &gt; ARP &gt; ARP Static Table.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>
<b>Monitoring Features</b>	
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	<p>Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP.</p> <p>This data is equivalent to the <b>show xlate count</b> command.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>

## New Features in ASA 8.4(4.1)/ASDM 6.4(9)

**Released: June 18, 2012**

[Table 16](#) lists the new features for ASA Version 8.4(4.1)/ASDM Version 6.4(9).



### Note

Version 8.4(4) was removed from Cisco.com due to build issues; please upgrade to Version 8.4(4.1) or later.

**Table 16**      **New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9)**

Feature	Description
<b>Certification Features</b>	
FIPS and Common Criteria certifications	<p>The FIPS 140-2 Non-Proprietary Security Policy was updated as part of the Level 2 FIPS 140-2 validation for the Cisco ASA 5500 series, which includes the Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580, and ASA 5585-X.</p> <p>The Common Criteria Evaluation Assurance Level 4 (EAL4) was updated, which provides the basis for a specific Target of Evaluation (TOE) of the Cisco ASA and VPN platform solutions.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>

**Table 16**      **New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9) (continued)**

Feature	Description
Support for administrator password policy when using the local database	<p>When you configure authentication for CLI or ASDM access using the local database, you can configure a password policy that requires a user to change their password after a specified amount of time and also requires password standards such as a minimum length and the minimum number of changed characters.</p> <p>We introduced or modified the following commands: <b>change-password</b>, <b>password-policy lifetime</b>, <b>password-policy minimum changes</b>, <b>password-policy minimum-length</b>, <b>password-policy minimum-lowercase</b>, <b>password-policy minimum-uppercase</b>, <b>password-policy minimum-numeric</b>, <b>password-policy minimum-special</b>, <b>password-policy authenticate enable</b>, <b>clear configure password-policy</b>, <b>show running-config password-policy</b>.</p> <p>We introduced the following screen: Configuration &gt; Device Management &gt; Users/AAA &gt; Password Policy</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>
Support for SSH public key authentication	<p>You can now enable public key authentication for SSH connections to the ASA on a per-user basis using Base64 key up to 2048 bits.</p> <p>We introduced the following commands: <b>ssh authentication</b>.</p> <p>We introduced the following screen: Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts &gt; Edit User Account &gt; Public Key Authentication</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>
Support for Diffie-Hellman Group 14 for the SSH Key Exchange	<p>Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported.</p> <p>We introduced the following command: <b>ssh key-exchange</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Management Access &gt; ASDM/HTTPS/Telnet/SSH.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>
Support for a maximum number of management sessions	<p>You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions.</p> <p>We introduced the following commands: <b>quota management-session</b>, <b>show running-config quota management-session</b>, <b>show quota management-session</b>.</p> <p>We introduced the following screen: Configuration &gt; Device Management &gt; Management Access &gt; Management Session Quota.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>

**Table 16**      **New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9) (continued)**

Feature	Description
Additional ephemeral Diffie-Hellman ciphers for SSL encryption	<p>The ASA now supports the following ephemeral Diffie-Hellman (DHE) SSL cipher suites:</p> <ul style="list-style-type: none"> <li>• DHE-AES128-SHA1</li> <li>• DHE-AES256-SHA1</li> </ul> <p>These cipher suites are specified in RFC 3268, <i>Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)</i>.</p> <p>When supported by the client, DHE is the preferred cipher because it provides Perfect Forward Secrecy. See the following limitations:</p> <ul style="list-style-type: none"> <li>• DHE is not supported on SSL 3.0 connections, so make sure to also enable TLS 1.0 for the SSL server.</li> </ul> <pre>!! set server version hostname(config)# <b>ssl server-version tlsv1 sslv3</b> !! set client version hostname(config) # <b>ssl client-version any</b></pre> <ul style="list-style-type: none"> <li>• Some popular applications do not support DHE, so include at least one other SSL encryption method to ensure that a cipher suite common to both the SSL client and server can be used.</li> <li>• Some clients may not support DHE, including AnyConnect 2.5 and 3.0, Cisco Secure Desktop, and Internet Explorer 9.0.</li> </ul> <p>We modified the following command: <b>ssl encryption</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Advanced &gt; SSL Settings.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>
Image verification	<p>Support for SHA-512 image integrity checking was added.</p> <p>We modified the following command: <b>verify</b>.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>
Improved pseudo-random number generation	<p>Hardware-based noise for additional entropy was added to the software-based random number generation process. This change makes pseudo-random number generation (PRNG) more random and more difficult for attackers to get a repeatable pattern or guess the next random number to be used for encryption and decryption operations. Two changes were made to improve PRNG:</p> <ul style="list-style-type: none"> <li>• Use the current hardware-based RNG for random data to use as one of the parameters for software-based RNG.</li> <li>• If the hardware-based RNG is not available, use additional hardware noise sources for software-based RNG. Depending on your model, the following hardware sensors are used: <ul style="list-style-type: none"> <li>– ASA 5505—Voltage sensors.</li> <li>– ASA 5510 and 5550—Fan speed sensors.</li> <li>– ASA 5520, 5540, and 5580—Temperature sensors.</li> <li>– ASA 5585-X—Fan speed sensors.</li> </ul> </li> </ul> <p>We introduced the following commands: <b>show debug menu cts [128   129]</b></p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).</i></p>

**Table 16**      **New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9) (continued)**

Feature	Description
<b>Remote Access Features</b>	
Clientless SSL VPN: Enhanced quality for rewriter engines	<p>The clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN users.</p> <p>We did not add or modify any commands for this feature.</p> <p>We did not add or modify any ASDM screens for this feature.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>
<b>Failover Features</b>	
Configure the connection replication rate during a bulk sync	<p>You can now configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASA is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synced.</p> <p>We introduced the following command: <b>failover replication rate</b> <i>rate</i>.</p> <p><i>This feature is not available in 8.6(1) or 8.7(1). This feature is also in 8.5(1.7).</i></p>
<b>Application Inspection Features</b>	
SunRPC change from dynamic ACL to pin-hole mechanism	<p>Previously, Sun RPC inspection does not support outbound access lists because the inspection engine uses dynamic access lists instead of secondary connections.</p> <p>In this release, when you configure dynamic access lists on the ASA, they are supported on the ingress direction only and the ASA drops egress traffic destined to dynamic ports. Therefore, Sun RPC inspection implements a pinhole mechanism to support egress traffic. Sun RPC inspection uses this pinhole mechanism to support outbound dynamic access lists.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>
Inspection reset action change	<p>Previously, when the ASA dropped a packet due to an inspection engine rule, the ASA sent only one RST to the source device of the dropped packet. This behavior could cause resource issues.</p> <p>In this release, when you configure an inspection engine to use a reset action and a packet triggers a reset, the ASA sends a TCP reset under the following conditions:</p> <ul style="list-style-type: none"> <li>• The ASA sends a TCP reset to the inside host when the <b>service resetoutbound</b> command is enabled. (The <b>service resetoutbound</b> command is disabled by default.)</li> <li>• The ASA sends a TCP reset to the outside host when the <b>service resetinbound</b> command is enabled. (The <b>service resetinbound</b> command is disabled by default.)</li> </ul> <p>For more information, see the <b>service</b> command in the <i>ASA Cisco ASA 5500 Series Command Reference</i>.</p> <p>This behavior ensures that a reset action will reset the connections on the ASA and on inside servers; therefore countering denial of service attacks. For outside hosts, the ASA does not send a reset by default and information is not revealed through a TCP reset.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>

**Table 16** *New Features for ASA Version 8.4(4.1)/ASDM Version 6.4(9) (continued)*

Feature	Description
<b>Module Features</b>	
ASA 5585-X support for the ASA CX SSP-10 and -20	<p>The ASA CX module lets you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees.</p> <p>We introduced or modified the following commands: <b>capture</b>, <b>cxsc</b>, <b>cxsc auth-proxy</b>, <b>debug cxsc</b>, <b>hw-module module password-reset</b>, <b>hw-module module reload</b>, <b>hw-module module reset</b>, <b>hw-module module shutdown</b>, <b>session do setup host ip</b>, <b>session do get-config</b>, <b>session do password-reset</b>, <b>show asp table classify domain cxsc</b>, <b>show asp table classify domain cxsc-auth-proxy</b>, <b>show capture</b>, <b>show conn</b>, <b>show module</b>, <b>show service-policy</b>.</p> <p>We introduced the following screens:</p> <p>Home &gt; ASA CX Status  Wizards &gt; Startup Wizard &gt; ASA CX Basic Configuration  Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule &gt; Rule Actions &gt; ASA CX Inspection</p>
ASA 5585-X support for network modules	<p>The ASA 5585-X now supports additional interfaces on network modules in slot 1. You can install one or two of the following optional network modules:</p> <ul style="list-style-type: none"> <li>• ASA 4-port 10G Network Module</li> <li>• ASA 8-port 10G Network Module</li> <li>• ASA 20-port 1G Network Module</li> </ul> <p><i>This feature is not available in 9.0(1), 9.0(2), or 9.1(1).</i></p>

## New Features in ASA 8.4(3)/ASDM 6.4(7)

**Released: January 9, 2012**

[Table 17](#) lists the new features for ASA Version 8.4(3)/ASDM Version 6.4(7).

**Table 17** *New Features for ASA Version 8.4(3)/ASDM Version 6.4(7)*

Feature	Description
<b>NAT Features</b>	
Round robin PAT pool allocation uses the same IP address for existing hosts	<p>When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available.</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p> <p><i>This feature is not available in 8.5(1) or 8.6(1).</i></p>



**Table 17**      **New Features for ASA Version 8.4(3)/ASDM Version 6.4(7) (continued)**

Feature	Description
Flat range of PAT ports for a PAT pool	<p>If available, the real source port number is used for the mapped port. However, if the real port is <i>not</i> available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool.</p> <p>If you have a lot of traffic that uses the lower port ranges, when using a PAT pool, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535.</p> <p>We modified the following commands: <b>nat dynamic</b> [<b>pat-pool</b> <i>mapped_object</i> [<b>flat</b> [<b>include-reserve</b>]]] (object network configuration mode) and <b>nat source dynamic</b> [<b>pat-pool</b> <i>mapped_object</i> [<b>flat</b> [<b>include-reserve</b>]]] (global configuration mode).</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object  Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule</p> <p><i>This feature is not available in 8.5(1) or 8.6(1).</i></p>
Extended PAT for a PAT pool	<p>Each PAT IP address allows up to 65535 ports. If 65535 ports do not provide enough translations, you can now enable extended PAT for a PAT pool. Extended PAT uses 65535 ports per <i>service</i>, as opposed to per IP address, by including the destination address and port in the translation information.</p> <p>We modified the following commands: <b>nat dynamic</b> [<b>pat-pool</b> <i>mapped_object</i> [<b>extended</b>]] (object network configuration mode) and <b>nat source dynamic</b> [<b>pat-pool</b> <i>mapped_object</i> [<b>extended</b>]] (global configuration mode).</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object  Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule</p> <p><i>This feature is not available in 8.5(1) or 8.6(1).</i></p>
Configurable timeout for PAT xlate	<p>When a PAT xlate times out (by default after 30 seconds), and the ASA reuses the port for a new translation, some upstream routers might reject the new connection because the previous connection might still be open on the upstream device. The PAT xlate timeout is now configurable, to a value between 30 seconds and 5 minutes.</p> <p>We introduced the following command: <b>timeout pat-xlate</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</p> <p><i>This feature is not available in 8.5(1) or 8.6(1).</i></p>

Table 17 New Features for ASA Version 8.4(3)/ASDM Version 6.4(7) (continued)

Feature	Description
Automatic NAT rules to translate a VPN peer's local IP address back to the peer's real IP address	<p>In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address.</p> <p>You can enable this feature on one interface per tunnel group. Object NAT rules are dynamically added and deleted when the VPN session is established or disconnected. You can view the rules using the <b>show nat</b> command.</p> <p><b>Note</b> Because of routing issues, we do not recommend using this feature unless you know you need this feature; contact Cisco TAC to confirm feature compatibility with your network. See the following limitations:</p> <ul style="list-style-type: none"> <li>• Only supports Cisco IPsec and AnyConnect Client.</li> <li>• Return traffic to the public IP addresses must be routed back to the ASA so the NAT policy and VPN policy can be applied.</li> <li>• Does not support load-balancing (because of routing issues).</li> <li>• Does not support roaming (public IP changing).</li> </ul> <p>We introduced the following command: <b>nat-assigned-to-public-ip interface</b> (tunnel-group general-attributes configuration mode).</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p>
<b>Remote Access Features</b>	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4.
Compression for DTLS and TLS	<p>To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients.</p> <p><b>Note</b> Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced.</p> <p>We introduced or modified the following commands: <b>anyconnect dtls compression [lzs   none]</b> and <b>anyconnect ssl compression [deflate   lzs   none]</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Group Policies &gt; Edit &gt; Edit Internal Group Policy &gt; Advanced &gt; AnyConnect Client &gt; SSL Compression.</p>

**Table 17**      **New Features for ASA Version 8.4(3)/ASDM Version 6.4(7) (continued)**

Feature	Description
Clientless SSL VPN Session Timeout Alerts	<p>Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout.</p> <p>We introduced the following commands: <b>vpn-session-timeout alert-interval</b>, <b>vpn-idle-timeout alert-interval</b>.</p> <p>We introduced the following screens:</p> <p>Remote Access VPN &gt; Configuration &gt; Clientless SSL VPN Access &gt; Portal &gt; Customizations &gt; Add/Edit &gt; Timeout Alerts</p> <p>Remote Access VPN &gt; Configuration &gt; Clientless SSL VPN Access &gt; Group Policies &gt; Add/Edit General</p>
<b>AAA Features</b>	
Increased maximum LDAP values per attribute	<p>The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037.</p> <p>We introduced the following command: <b>ldap-max-value-range number</b> (Enter this command in aaa-server host configuration mode).</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p>
Support for sub-range of LDAP search results	<p>When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.</p>
Key vendor-specific attributes (VSAs) sent in RADIUS access request and accounting request packets from the ASA	<p>Four New VSAs—Tunnel Group Name (146) and Client Type (150) are sent in RADIUS access request packets from the ASA. Session Type (151) and Session Subtype (152) are sent in RADIUS accounting request packets from the ASA. All four attributes are sent for all accounting request packet types: Start, Interim-Update, and Stop. The RADIUS server (for example, ACS and ISE) can then enforce authorization and policy attributes or use them for accounting and billing purposes.</p>
<b>Troubleshooting Features</b>	
Regular expression matching for the <b>show asp table classifier</b> and <b>show asp table filter</b> commands	<p>You can now enter the <b>show asp table classifier</b> and <b>show asp table filter</b> commands with a regular expression to filter output.</p> <p>We modified the following commands: <b>show asp table classifier match regex</b>, <b>show asp table filter match regex</b>.</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p>

## New Features in ASA 8.4(2.8)/ASDM 6.4(5.106)

Released: August 31, 2011

Table 18 lists the new features for ASA interim Version 8.4(2.8)/ASDM Version 6.4(5.106).



#### Note

We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

**Table 18**      **New Features for ASA Interim Version 8.4(2.8)/ASDM Version 6.4(5.106)**

Feature	Description
<b>Remote Access Features</b>	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. <i>Also available in Version 8.2(5.13) and 8.3.2(25).</i>
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients.  <b>Note</b> Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced.  We introduced or modified the following commands: <b>anyconnect dtls compression [lzs   none]</b> and <b>anyconnect ssl compression [deflate   lzs   none]</b> .  We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConnect Client > SSL Compression.  <i>Also available in Version 8.2(5.13) and 8.3.2(25).</i>
Clientless SSL VPN Session Timeout Alerts	Allows you to create custom messages to alert users that their VPN session is about to end because of inactivity or a session timeout.  We introduced the following commands: <b>vpn-session-timeout alert-interval</b> , <b>vpn-idle-timeout alert-interval</b> .  We introduced the following screens:  Remote Access VPN > Configuration > Clientless SSL VPN Access > Portal > Customizations > Add/Edit > Timeout Alerts Remote Access VPN > Configuration > Clientless SSL VPN Access > Group Policies > Add/Edit General
<b>AAA Features</b>	

**Table 18**      **New Features for ASA Interim Version 8.4(2.8)/ASDM Version 6.4(5.106) (continued)**

Feature	Description
Increased maximum LDAP values per attribute	<p>The maximum number of values that the ASA can receive for a single attribute was increased from 1000 (the default) to 5000, with an allowed range of 500 to 5000. If a response message is received that exceeds the configured limit, the ASA rejects the authentication. If the ASA detects that a single attribute has more than 1000 values, then the ASA generates informational syslog 109036. For more than 5000 attributes, the ASA generates error level syslog 109037.</p> <p>We introduced the following command: <b>ldap-max-value-range</b> <i>number</i> (Enter this command in aaa-server host configuration mode).</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p>
Support for sub-range of LDAP search results	<p>When an LDAP search results in an attribute with a large number of values, depending on the server configuration, it might return a sub-range of the values and expect the ASA to initiate additional queries for the remaining value ranges. The ASA now makes multiple queries for the remaining ranges, and combines the responses into a complete array of attribute values.</p>
<b>Troubleshooting Features</b>	
Regular expression matching for the <b>show asp table classifier</b> and <b>show asp table filter</b> commands	<p>You can now enter the <b>show asp table classifier</b> and <b>show asp table filter</b> commands with a regular expression to filter output.</p> <p>We modified the following commands: <b>show asp table classifier match</b> <i>regex</i>, <b>show asp table filter match</b> <i>regex</i>.</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p> <p><i>Also available in Version 8.2(5.13) and 8.3.2(25).</i></p>

## New Features in ASA 8.4(2)/ASDM 6.4(5)

Released: June 20, 2011

Table 19 lists the new features for ASA Version 8.4(2)/ASDM Version 6.4(5).

**Table 19**      **New Features for ASA Version 8.4(2)/ASDM Version 6.4(5)**

Feature	Description
<b>Firewall Features</b>	
Identity Firewall	<p>Typically, a firewall is not aware of the user identities and, therefore, cannot apply security policies based on identity.</p> <p>The Identity Firewall in the ASA provides more granular access control based on users' identities. You can configure access rules and security policies based on usernames and user groups name rather than through source IP addresses. The ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped usernames instead of network IP addresses.</p> <p>The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping. The ASA uses Windows Active Directory as the source to retrieve the current user identity information for specific IP addresses.</p> <p>In an enterprise, some users log onto the network by using other authentication mechanisms, such as authenticating with a web portal (cut-through proxy) or by using a VPN. You can configure the Identity Firewall to allow these types of authentication in connection with identity-based access policies.</p> <p>We introduced or modified the following commands: <b>user-identity enable</b>, <b>user-identity default-domain</b>, <b>user-identity domain</b>, <b>user-identity logout-probe</b>, <b>user-identity inactive-user-timer</b>, <b>user-identity poll-import-user-group-timer</b>, <b>user-identity action netbios-response-fail</b>, <b>user-identity user-not-found</b>, <b>user-identity action ad-agent-down</b>, <b>user-identity action mac-address-mismatch</b>, <b>user-identity action domain-controller-down</b>, <b>user-identity ad-agent active-user-database</b>, <b>user-identity ad-agent hello-timer</b>, <b>user-identity ad-agent aaa-server</b>, <b>user-identity update import-user</b>, <b>user-identity static user</b>, <b>ad-agent-mode</b>, <b>dns domain-lookup</b>, <b>dns poll-timer</b>, <b>dns expire-entry-timer</b>, <b>object-group user</b>, <b>show user-identity</b>, <b>show dns</b>, <b>clear configure user-identity</b>, <b>clear dns</b>, <b>debug user-identity</b>, <b>test aaa-server ad-agent</b>.</p> <p>We introduced the following screens:</p> <p>Configuration &gt; Firewall &gt; Identity Options.  Configuration &gt; Firewall &gt; Objects &gt; Local User Groups  Monitoring &gt; Properties &gt; Identity</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Users/AAA &gt; AAA Server Groups &gt; Add/Edit Server Group.</p>

**Table 19**      **New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)**

Feature	Description
Identity NAT configurable proxy ARP and route lookup	<p>In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was always used to determine the egress interface. You could not configure these settings. In 8.4(2) and later, the default behavior for identity NAT was changed to match the behavior of other static NAT configurations: proxy ARP is enabled, and the NAT configuration determines the egress interface (if specified) by default. You can leave these settings as is, or you can enable or disable them discretely. Note that you can now also disable proxy ARP for regular static NAT.</p> <p>For pre-8.3 configurations, the migration of NAT exempt rules (the <b>nat 0 access-list</b> command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: <b>no-proxy-arp</b> and <b>route-lookup</b>. The <b>unidirectional</b> keyword that was used for migrating to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the <b>no-proxy-arp</b> and <b>route-lookup</b> keywords, to maintain existing functionality. The <b>unidirectional</b> keyword is removed.</p> <p>We modified the following commands: <b>nat static [no-proxy-arp] [route-lookup]</b> (object network) and <b>nat source static [no-proxy-arp] [route-lookup]</b> (global).</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object &gt; Advanced NAT Settings Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule</p>
PAT pool and round robin address assignment	<p>You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy.</p> <p><b>Note</b>    Currently in 8.4(2), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634).</p> <p>We modified the following commands: <b>nat dynamic [pat-pool mapped_object [round-robin]]</b> (object network) and <b>nat source dynamic [pat-pool mapped_object [round-robin]]</b> (global).</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule</p>

**Table 19**      ***New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)***

Feature	Description
IPv6 Inspection	<p>You can configure IPv6 inspection by configuring a service policy to selectively block IPv6 traffic based on the extension header. IPv6 packets are subjected to an early security check. The ASA always passes hop-by-hop and destination option types of extension headers while blocking router header and no next header.</p> <p>You can enable default IPv6 inspection or customize IPv6 inspection. By defining a policy map for IPv6 inspection you can configure the ASA to selectively drop IPv6 packets based on following types of extension headers found anywhere in the IPv6 packet:</p> <ul style="list-style-type: none"> <li>• Hop-by-Hop Options</li> <li>• Routing (Type 0)</li> <li>• Fragment</li> <li>• Destination Options</li> <li>• Authentication</li> <li>• Encapsulating Security Payload</li> </ul> <p>We modified the following commands: <b>policy-map type inspect ipv6, verify-header, match header, match header routing-type, match header routing-address count gt, match header count gt</b>.</p> <p>We introduced the following screen: Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; IPv6.</p>
<b>Remote Access Features</b>	
Portal Access Rules	<p>This enhancement allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in the HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources.</p> <p>We modified the following command: <b>webvpn portal-access-rule</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Portal Access Rules.</p> <p><i>Also available in Version 8.2(5).</i></p>
Clientless support for Microsoft Outlook Web App 2010	<p>The ASA 8.4(2) clientless SSL VPN core rewriter now supports Microsoft Outlook Web App 2010.</p>
Secure Hash Algorithm SHA-2 Support for IPsec IKEv2 Integrity and PRF	<p>This release supports the Secure Hash Algorithm SHA-2 for increased cryptographic hashing security for IPsec/IKEv2 AnyConnect Secure Mobility Client connections to the ASA. SHA-2 includes hash functions with digests of 256, 384, or 512 bits, to meet U.S. government requirements.</p> <p>We modified the following commands: <b>integrity, prf, show crypto ikev2 sa detail, show vpn-sessiondb detail remote</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; IPsec &gt; IKE Policies &gt; Add/Edit IKEv2 Policy (Proposal).</p>



**Table 19**      **New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)**

Feature	Description
Secure Hash Algorithm SHA-2 Support for Digital Signature over IPsec IKEv2	<p>This release supports the use of SHA-2 compliant signature algorithms to authenticate IPsec IKEv2 VPN connections that use digital certificates, with the hash sizes SHA-256, SHA-384, and SHA-512.</p> <p>SHA-2 digital signature for IPsec IKEv2 connections is supported with the AnyConnect Secure Mobility Client, Version 3.0.1 or later.</p>
Split Tunnel DNS policy for AnyConnect	<p>This release includes a new policy pushed down to the AnyConnect Secure Mobility Client for resolving DNS addresses over split tunnels. This policy applies to VPN connections using the SSL or IPsec/IKEv2 protocol and instructs the AnyConnect client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyConnect client does not try to resolve the address through public DNS servers.</p> <p>By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy: tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list.</p> <p>We introduced the following command: <b>split-tunnel-all-dns</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; Add/Edit Group Policy &gt; Advanced &gt; Split Tunneling (see the Send All DNS Lookups Through Tunnel check box).</p> <p><i>Also available in Version 8.2(5).</i></p>

**Table 19**      **New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)**

Feature	Description
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	<p>You can now configure the ASA to permit or deny VPN connections to mobile devices, enable or disable mobile device access on a per group bases, and gather information about connected mobile devices based on a mobile device's posture data. The following mobile platforms support this capability: AnyConnect for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Android Version 2.4.x.</p> <p><b>Licensing Requirements</b></p> <p>Enforcing remote access controls and gathering posture data from mobile devices requires an AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to be installed on the ASA. You receive the following functionality based on the license you install:</p> <ul style="list-style-type: none"> <li>• <b>AnyConnect Premium License Functionality</b> Enterprises that install the AnyConnect Premium license will be able to enforce DAP policies, on supported mobile devices, based on these DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device.</li> <li>• <b>AnyConnect Essentials License Functionality</b> Enterprises that install the AnyConnect Essentials license will be able to do the following: <ul style="list-style-type: none"> <li>– Enable or disable mobile device access on a per group basis and to configure that feature using ASDM.</li> <li>– Display information about connected mobile devices via CLI or ASDM without having the ability to enforce DAP policies or deny or allow remote access to those mobile devices.</li> </ul> </li> </ul> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Dynamic Access Policies &gt; Add/Edit Endpoint Attributes &gt; Endpoint Attribute Type:AnyConnect.</p> <p><i>Also available in Version 8.2(5).</i></p>
SSL SHA-2 digital signature	<p>You can now use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5(1) or later (2.5(2) or later recommended). This release does not support SHA-2 for other uses or products.</p> <p>Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image.</p> <p>We modified the following command: <b>show crypto ca certificate</b> (the Signature Algorithm field identifies the digest algorithm used when generating the signature).</p> <p>We did not modify any screens.</p> <p><i>Also available in Version 8.2(5).</i></p>
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	<p>ASA supports SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients when using the L2TP/IPsec protocol.</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p> <p><i>Also available in Version 8.2(5).</i></p>

**Table 19**      **New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)**

Feature	Description
Enable/disable certificate mapping to override the group-url attribute	<p>This feature changes the preference of a connection profile during the connection profile selection process. By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This optional feature changes the preference to a connection profile that specifies the group URL requested by the endpoint. The new option lets administrators rely on the group URL preference used by many older ASA software releases.</p> <p>We introduced the following command: <b>tunnel-group-preference</b>.</p> <p>We modified the following screens:</p> <p>Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN &gt; Connection Profiles  Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles</p> <p><i>Also available in Version 8.2(5).</i></p>
<b>ASA 5585-X Features</b>	
Support for Dual SSPs for SSP-40 and SSP-60	<p>For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). Each SSP acts as an independent device, with separate configurations and management. You can use the two SSPs as a failover pair if desired.</p> <p><b>Note</b>    When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled.</p> <p>We modified the following commands: <b>show module</b>, <b>show inventory</b>, <b>show environment</b>.</p> <p>We did not modify any screens.</p>
Support for the IPS SSP-10, -20, -40, and -60	<p>We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10.</p> <p><i>Also available in Version 8.2(5).</i></p>
<b>CSC SSM Features</b>	
CSC SSM Support	<p>For the CSC SSM, support for the following features has been added:</p> <ul style="list-style-type: none"> <li>• HTTPS traffic redirection: URL filtering and WRS queries for incoming HTTPS connections.</li> <li>• Configuring global approved whitelists for incoming and outgoing SMTP and POP3 e-mail.</li> <li>• E-mail notification for product license renewals.</li> </ul> <p>We modified the following screens:</p> <p>Configuration &gt; Trend Micro Content Security &gt; Mail &gt; SMTP  Configuration &gt; Trend Micro Content Security &gt; Mail &gt; POP3  Configuration &gt; Trend Micro Content Security &gt; Host/Notification Settings  Configuration &gt; Trend Micro Content Security &gt; CSC Setup &gt; Host Configuration</p> <p>We did not modify any commands.</p>
<b>Monitoring Features</b>	

**Table 19**      **New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)**

Feature	Description
Smart Call-Home Anonymous Reporting	<p>Customers can now help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device.</p> <p>We introduced the following commands: <b>call-home reporting anonymous</b>, <b>call-home test reporting anonymous</b>.</p> <p>We modified the following screen: Configuration &gt; Device Monitoring &gt; Smart Call-Home.</p> <p><i>Also available in Version 8.2(5).</i></p>
IF-MIB ifAlias OID support	<p>The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will be set to the value that has been set for the interface description.</p> <p><i>Also available in Version 8.2(5).</i></p>
<b>Interface Features</b>	
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	<p>You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interfaces; support was previously added for 10-Gigabit Ethernet interfaces in 8.2(2).</p> <p>We modified the following command: <b>flowcontrol</b>.</p> <p>We modified the following screens:</p> <p>(Single Mode) Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface &gt; General (Multiple Mode, System) Configuration &gt; Interfaces &gt; Add/Edit Interface</p> <p><i>Also available in Version 8.2(5).</i></p>
<b>Management Features</b>	
Increased SSH security; the SSH default username is no longer supported	<p>Starting in 8.4(2), you can no longer connect to the ASA using SSH with the <b>pix</b> or <b>asa</b> username and the login password. To use SSH, you must configure AAA authentication using the <b>aaa authentication ssh console LOCAL</b> command (CLI) or Configuration &gt; Device Management &gt; Users/AAA &gt; AAA Access &gt; Authentication (ASDM); then define a local user by entering the <b>username</b> command (CLI) or choosing Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.</p>
<b>Unified Communications Features</b>	
ASA-Tandberg Interoperability with H.323 Inspection	<p>H.323 Inspection now supports uni-directional signaling for two-way video sessions. This enhancement allows H.323 Inspection of one-way video conferences supported by Tandberg video phones. Supporting uni-directional signaling allows Tandberg phones to switch video modes (close their side of an H.263 video session and reopen the session using H.264, the compression standard for high-definition video).</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p> <p><i>Also available in Version 8.2(5).</i></p>
<b>Routing Features</b>	

**Table 19**      **New Features for ASA Version 8.4(2)/ASDM Version 6.4(5) (continued)**

Feature	Description
Timeout for connections using a backup static route	<p>When multiple static routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value.</p> <p>We modified the following command: <b>timeout floating-conn</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</p> <p><i>Also available in Version 8.2(5).</i></p>
<b>ASDM Features</b>	
Migrate Network Object Group Members	<p>If you migrate to 8.3 or later, the ASA creates named network objects to replace inline IP addresses in some features. In addition to named objects, ASDM automatically creates non-named objects for any IP addresses used in the configuration. These auto-created objects are identified by the IP address only, do not have a name, and are not present as named objects in the platform configuration.</p> <p>When the ASA creates named objects as part of the migration, the matching non-named ASDM-only objects are replaced with the named objects. The only exception are non-named objects in a network object group. When the ASA creates named objects for IP addresses that are inside a network object group, ASDM retains the non-named objects as well, creating duplicate objects in ASDM. To merge these objects, choose <b>Tools &gt; Migrate Network Object Group Members</b>.</p> <p>We introduced the following screen: Tools &gt; Migrate Network Object Group Members.</p> <p>See <i>Cisco ASA 5500 Migration to Version 8.3 and Later</i> for more information.</p>

## New Features in ASA 8.4(1.11)/ASDM 6.4(2)

**Released: May 20, 2011**

[Table 20](#) lists the new features for ASA interim Version 8.4(1.11)/ASDM Version 6.4(2).



### Note

We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the interim release notes available on the Cisco.com software download site.

**Table 20**      ***New Features for ASA Version 8.4(1.11)/ASDM Version 6.4(2)***

Feature	Description
<b>Firewall Features</b>	
PAT pool and round robin address assignment	<p>You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy.</p> <p><b>Note</b>    Currently in 8.4(1.11), the PAT pool feature is not available as a fallback method for dynamic NAT or PAT. You can only configure the PAT pool as the primary method for dynamic PAT (CSCtq20634).</p> <p>We modified the following commands: <b>nat dynamic</b> [<b>pat-pool</b> <i>mapped_object</i> [<b>round-robin</b>]] (<i>object network</i>) and <b>nat source dynamic</b> [<b>pat-pool</b> <i>mapped_object</i> [<b>round-robin</b>]] (<i>global</i>).</p> <p>We modified the following screens:</p> <p>Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object  Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule</p>

## New Features in ASA 8.4(1)/ASDM 6.4(1)

Released: January 31, 2011

[Table 21](#) lists the new features for ASA Version 8.4(1)/ASDM Version 6.4(1).

**Table 21**      ***New Features for ASA Version 8.4(1)/ASDM Version 6.4(1)***

Feature	Description
<b>Hardware Features</b>	
Support for the ASA 5585-X	<p>We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10, -20, -40, and -60.</p> <p><b>Note</b>    Support was previously added in 8.2(3) and 8.2(4); the ASA 5585-X is not supported in 8.3(x).</p>
No Payload Encryption hardware for export	<p>You can purchase the ASA 5585-X with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. The ASA software senses a No Payload Encryption model, and disables the following features:</p> <ul style="list-style-type: none"> <li>Unified Communications</li> <li>VPN</li> </ul> <p>You can still install the Strong Encryption (3DES/AES) license for use with management connections. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL).</p>
<b>Remote Access Features</b>	

**Table 21**      **New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)**

Feature	Description
L2TP/IPsec Support on Android Platforms	<p>We now support VPN connections between Android mobile devices and ASA 5500 series devices, when using the L2TP/IPsec protocol and the native Android VPN client. Mobile devices must be using the Android 2.1, or later, operating system.</p> <p><i>Also available in Version 8.2(5).</i></p>
UTF-8 Character Support for AnyConnect Passwords	AnyConnect 3.0 used with ASA 8.4(1), supports UTF-8 characters in passwords sent using RADIUS/MSCHAP and LDAP protocols.
IPsec VPN Connections with IKEv2	<p>Internet Key Exchange Version 2 (IKEv2) is the latest key exchange protocol used to establish and control Internet Protocol Security (IPsec) tunnels. The ASA now supports IPsec with IKEv2 for the AnyConnect Secure Mobility Client, Version 3.0(1), for all client operating systems.</p> <p>On the ASA, you enable IPsec connections for users in the group policy. For the AnyConnect client, you specify the primary protocol (IPsec or SSL) for each ASA in the server list of the client profile.</p> <p>IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses.</p> <p>Site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). The Other VPN license is included in the Base license.</p> <p>We modified the following commands: <b>vpn-tunnel-protocol</b>, <b>crypto ikev2 policy</b>, <b>crypto ikev2 enable</b>, <b>crypto ipsec ikev2</b>, <b>crypto dynamic-map</b>, <b>crypto map</b>.</p> <p>We modified the following screens:</p> <ul style="list-style-type: none"> <li>Configure &gt; Site-to-Site VPN &gt; Connection Profiles</li> <li>Configure &gt; Remote Access &gt; Network (Client) Access &gt; AnyConnect Connection Profiles</li> <li>Network (Client) Access &gt; Advanced &gt; IPsec &gt; IKE Parameters &gt; IKE Policies</li> <li>Network (Client) Access &gt; Advanced &gt; IPsec &gt; IKE Parameters &gt; IKE Parameters</li> <li>Network (Client) Access &gt; Advanced &gt; IPsec &gt; IKE Parameters &gt; IKE Proposals</li> </ul>
SSL SHA-2 digital signature	<p>This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommended). This release does not support SHA-2 for other uses or products. This feature does not involve configuration changes.</p> <p><b>Caution:</b> To support failover of SHA-2 connections, the standby ASA must be running the same image. To support this feature, we added the Signature Algorithm field to the <b>show crypto ca certificate command</b> to identify the digest algorithm used when generating the signature.</p>
SCEP Proxy	<p>SCEP Proxy provides the AnyConnect Secure Mobility Client with support for automated third-party certificate enrollment. Use this feature to support AnyConnect with zero-touch, secure deployment of device certificates to authorize endpoint connections, enforce policies that prevent access by non-corporate assets, and track corporate assets. This feature requires an AnyConnect Premium license and will not work with an Essentials license.</p> <p>We introduced or modified the following commands: <b>crypto ikev2 enable</b>, <b>scep-enrollment enable</b>, <b>scep-forwarding-url</b>, <b>debug crypto ca scep-proxy</b>, <b>secondary-username-from-certificate</b>, <b>secondary-pre-fill-username</b>.</p>

**Table 21**      ***New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)***

<b>Feature</b>	<b>Description</b>
Host Scan Package Support	<p>This feature provides the necessary support for the ASA to install or upgrade a Host Scan package and enable or disable Host Scan. This package may either be a standalone Host Scan package or one that ASA extracts from an AnyConnect Next Generation package.</p> <p>In previous releases of AnyConnect, an endpoint's posture was determined by Cisco Secure Desktop (CSD). Host Scan was one of many features bundled in CSD. Unbundling Host Scan from CSD gives AnyConnect administrators greater freedom to update and install Host Scan separately from the other features of CSD.</p> <p>We introduced the following command: <b>csd hostscan image path</b>.</p>
Kerberos Constrained Delegation (KCD)	<p>This release implements the KCD protocol transition and constrained delegation extensions on the ASA. KCD provides Clientless SSL VPN (also known as WebVPN) users with SSO access to any web services protected by Kerberos. Examples of such services or applications include Outlook Web Access (OWA), Sharepoint, and Internet Information Server (IIS).</p> <p>Implementing protocol transition allows the ASA to obtain Kerberos service tickets on behalf of remote access users without requiring them to authenticate to the KDC (through Kerberos). Instead, a user authenticates to ASA using any of the supported authentication mechanisms, including digital certificates and Smartcards, for Clientless SSL VPN (also known as WebVPN). When user authentication is complete, the ASA requests and obtains an impersonate ticket, which is a service ticket for ASA on behalf of the user. The ASA may then use the impersonate ticket to obtain other service tickets for the remote access user.</p> <p>Constrained delegation provides a way for domain administrators to limit the network resources that a service trusted for delegation (for example, the ASA) can access. This task is accomplished by configuring the account under which the service is running to be trusted for delegation to a specific instance of a service running on a specific computer.</p> <p>We modified the following commands: <b>kcd-server</b>, <b>clear aaa</b>, <b>show aaa</b>, <b>test aaa-server authentication</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Advanced &gt; Microsoft KCD Server.</p>
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Apple Safari 5.



**Table 21**      **New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)**

Feature	Description
Clientless VPN Auto Sign-on Enhancement	<p>Smart tunnel now supports HTTP-based auto sign-on on Firefox as well as Internet Explorer. Similar to when Internet Explorer is used, the administrator decides to which hosts a Firefox browser will automatically send credentials. For some authentication methods, it may be necessary for the administrator to specify a realm string on the ASA to match that on the web application (in the Add Smart Tunnel Auto Sign-on Server window). You can now use bookmarks with macro substitutions for auto sign-on with Smart tunnel as well.</p> <p>The POST plug-in is now obsolete. The former POST plug-in was created so that administrators could specify a bookmark with sign-on macros and receive a kick-off page to load prior to posting the the POST request. The POST plug-in approach allows requests that required the presence of cookies, and other header items, fetched ahead of time to go through. The administrator can now specify pre-load pages when creating bookmarks to achieve the same functionality. Same as the POST plug-in, the administrator specifies the pre-load page URL and the URL to send the POST request to.</p> <p>You can now replace the default preconfigured SSL VPN portal with your own portal. The administrators do this by specifying a URL as an External Portal. Unlike the group-policy home page, the External Portal supports POST requests with macro substitution (for auto sign-on) as well as pre-load pages.</p> <p>We introduced or modified the following command: <b>smart-tunnel auto-signon</b>.</p> <p>We introduced or modified the following screens:  Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Customization.  Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Bookmarks &gt; Edit &gt; Edit Bookmark</p>
Expanded Smart Tunnel application support	<p>Smart Tunnel adds support for the following applications:</p> <ul style="list-style-type: none"> <li>Microsoft Outlook Exchange Server 2010 (native support). Users can now use Smart Tunnel to connect Microsoft Office Outlook to a Microsoft Exchange Server.</li> <li>Microsoft Sharepoint/Office 2010. Users can now perform remote file editing using Microsoft Office 2010 Applications and Microsoft Sharepoint by using Smart Tunnel.</li> </ul>
<b>Interface Features</b>	
EtherChannel support (ASA 5510 and higher)	<p>You can configure up to 48 802.3ad EtherChannels of eight active interfaces each.</p> <p><b>Note</b> You cannot use interfaces on the 4GE SSM, including the integrated 4GE SSM in slot 1 on the ASA 5550, as part of an EtherChannel.</p> <p>We introduced the following commands: <b>channel-group</b>, <b>lACP port-priority</b>, <b>interface port-channel</b>, <b>lACP max-bundle</b>, <b>port-channel min-bundle</b>, <b>port-channel load-balance</b>, <b>lACP system-priority</b>, <b>clear lACP counters</b>, <b>show lACP</b>, <b>show port-channel</b>.</p> <p>We introduced or modified the following screens:  Configuration &gt; Device Setup &gt; Interfaces  Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit EtherChannel Interface  Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface  Configuration &gt; Device Setup &gt; EtherChannel</p>

**Table 21**      ***New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)***

<b>Feature</b>	<b>Description</b>
Bridge groups for transparent mode	<p>If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups. You can configure up to 8 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group.</p> <p><b>Note</b> Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group.</p> <p>We introduced the following commands: <b>interface bvi</b>, <b>bridge-group</b>, <b>show bridge-group</b>.</p> <p>We modified or introduced the following screens:            Configuration &gt; Device Setup &gt; Interfaces            Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Bridge Group Interface            Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface</p>
<b>Scalability Features</b>	
Increased contexts for the ASA 5550, 5580, and 5585-X	For the ASA 5550 and ASA 5585-X with SSP-10, the maximum contexts was increased from 50 to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was increased from 50 to 250.
Increased VLANs for the ASA 5580 and 5585-X	For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.
Additional platform support	Google Chrome has been added as a supported platform for ASA Version 8.4. Both 32-bit and 64-bit platforms are supported on Windows XP, Vista, and 7 and Mac OS X Version 6.0.
Increased connections for the ASA 5580 and 5585-X	<p>We increased the firewall connection limits:</p> <ul style="list-style-type: none"> <li>ASA 5580-20—1,000,000 to 2,000,000.</li> <li>ASA 5580-40—2,000,000 to 4,000,000.</li> <li>ASA 5585-X with SSP-10: 750,000 to 1,000,000.</li> <li>ASA 5585-X with SSP-20: 1,000,000 to 2,000,000.</li> <li>ASA 5585-X with SSP-40: 2,000,000 to 4,000,000.</li> <li>ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.</li> </ul>
Increased AnyConnect VPN sessions for the ASA 5580	The AnyConnect VPN session limit was increased from 5,000 to 10,000.
Increased Other VPN sessions for the ASA 5580	The other VPN session limit was increased from 5,000 to 10,000.
<b>High Availability Features</b>	
Stateful Failover with Dynamic Routing Protocols	<p>Routes that are learned through dynamic routing protocols (such as OSPF and EIGRP) on the active unit are now maintained in a Routing Information Base (RIB) table on the standby unit. Upon a failover event, traffic on the secondary active unit now passes with minimal disruption because routes are known. Routes are synchronized only for link-up or link-down events on an active unit. If the link goes up or down on the standby unit, dynamic routes sent from the active unit may be lost. This is normal, expected behavior.</p> <p>We modified the following commands: <b>show failover</b>, <b>show route</b>, <b>show route failover</b>.</p> <p>We did not modify any screens.</p>

**Table 21**      **New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)**

Feature	Description
<b>Unified Communication Features</b>	
Phone Proxy addition to Unified Communication Wizard	<p>The Unified Communications wizard guides you through the complete configuration and automatically configures required aspects for the Phone Proxy. The wizard automatically creates the necessary TLS proxy, then guides you through creating the Phone Proxy instance, importing and installing the required certificates, and finally enables the SIP and SCCP inspection for the Phone Proxy traffic automatically.</p> <p>We modified the following screens: Wizards &gt; Unified Communications Wizard. Configuration &gt; Firewall &gt; Unified Communications.</p>
UC Protocol Inspection Enhancements	<p>SIP Inspection and SCCP Inspection are enhanced to support new features in the Unified Communications Solutions; such as, SCCP v2.0 support, support for GETPORT messages in SCCP Inspection, SDP field support in INVITE messages with SIP Inspection, and QSIG tunneling over SIP. Additionally, the Cisco Intercompany Media Engine supports Cisco RT Lite phones and third-party video endpoints (such as, Tandberg).</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p>
<b>Inspection Features</b>	
DCERPC Enhancement	<p>DCERPC Inspection was enhanced to support inspection of RemoteCreateInstance RPC messages.</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p>
<b>Troubleshooting and Monitoring Features</b>	
SNMP traps and MIBs	<p>Supports the following additional keywords: <b>connection-limit-reached, entity cpu-temperature, cpu threshold rising, entity fan-failure, entity power-supply, ikev2 stop   start, interface-threshold, memory-threshold, nat packet-discard, warmstart</b>.</p> <p>The entPhysicalTable reports entries for sensors, fans, power supplies, and related components.</p> <p>Supports the following additional MIBs: ENTITY-SENSOR-MIB, CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, NAT-MIB, EVENT-MIB, EXPRESSION-MIB</p> <p>Supports the following additional traps: warmstart, cpmCPURisingThreshold, mteTriggerFired, cirResourceLimitReached, natPacketDiscard, ciscoEntSensorExtThresholdNotification.</p> <p>We introduced or modified the following commands: <b>snmp cpu threshold rising, snmp interface threshold, snmp-server enable traps</b>.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; Management Access &gt; SNMP.</p>

**Table 21**      ***New Features for ASA Version 8.4(1)/ASDM Version 6.4(1) (continued)***

<b>Feature</b>	<b>Description</b>
TCP Ping Enhancement	<p>TCP ping allows users whose ICMP echo requests are blocked to check connectivity over TCP. With the TCP ping enhancement you can specify a source IP address and a port and source interface to send pings to a hostname or an IPv4 address.</p> <p>We modified the following command: <b>ping tcp</b>.</p> <p>We modified the following screen: Tools &gt; Ping.</p>
Show Top CPU Processes	<p>You can now monitor the processes that run on the CPU to obtain information related to the percentage of the CPU used by any given process. You can also see information about the load on the CPU, broken down per process, at 5 minutes, 1 minute, and 5 seconds prior to the log time. Information is updated automatically every 5 seconds to provide real-time statistics, and a refresh button in the pane allows a manual data refresh at any time.</p> <p>We introduced the following command: <b>show process cpu-usage sorted</b>.</p> <p>We introduced the following screen: Monitoring &gt; Properties &gt; CPU - Per Process.</p>
<b>General Features</b>	
Password Encryption Visibility	<p>You can show password encryption in a security context.</p> <p>We modified the following command: <b>show password encryption</b>.</p> <p>We did not modify any screens.</p>
<b>ASDM Features</b>	
ASDM Upgrade Enhancement	<p>When ASDM loads on a device that has an incompatible ASA software version, a dialog box notifies users that they can select from the following options:</p> <ul style="list-style-type: none"> <li>• Upgrade the image version from Cisco.com.</li> <li>• Upgrade the image version from their local drive.</li> <li>• Continue with the incompatible ASDM/ASA pair (new choice).</li> </ul> <p>We did not modify any screens.</p> <p>This feature interoperates with all ASA versions.</p>
Implementing IKEv2 in Wizards	<p>IKEv2 support has been implemented into the AnyConnect VPN Wizard (formerly SSL VPN wizard), the Clientless SSL VPN Wizard, and the Site-to-Site IPsec VPN Wizard (formerly IPsec VPN Wizard) to comply with IPsec remote access requirements defined in federal and public sector mandates. Along with the enhanced security, the new support offers the same end user experience independent of the tunneling protocol used by the AnyConnect client session. IKEv2 also allows other vendors' VPN clients to connect to the ASAs.</p> <p>We modified the following wizards: Site-to-Site IPsec VPN Wizard, AnyConnect VPN Wizard, and Clientless SSL VPN Wizard.</p>
IPS Startup Wizard enhancements	<p>For the IPS SSP in the ASA 5585-X, the IPS Basic Configuration screen was added to the startup wizard. Signature updates for the IPS SSP were also added to the Auto Update screen. The Time Zone and Clock Configuration screen was added to ensure the clock is set on the ASA; the IPS SSP gets its clock from the ASA.</p> <p>We introduced or modified the following screens:</p> <p>Wizards &gt; Startup Wizard &gt; IPS Basic Configuration</p> <p>Wizards &gt; Startup Wizard &gt; Auto Update</p> <p>Wizards &gt; Startup Wizard &gt; Time Zone and Clock Configuration</p>

# New Features in Version 8.3

This section includes the following topics:

- [New Features in ASA 8.3\(2.25\)/ASDM 6.4\(5.106\), page 70](#)
- [New Features in ASA 8.3\(2\)/ASDM 6.3\(2\), page 71](#)
- [New Features in ASA 8.3\(1\)/ASDM 6.3\(1\), page 73](#)

## New Features in ASA 8.3(2.25)/ASDM 6.4(5.106)

**Released: August 31, 2011**

[Table 18](#) lists the new features for ASA interim Version 8.3(2.25)/ASDM Version 6.4(5.106).



### Note

We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

**Table 22**      **New Features for ASA Interim Version 8.3(2.25)/ASDM Version 6.4(5.106)**

Feature	Description
<b>Remote Access Features</b>	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. <i>Also available in Version 8.2(5.13) and 8.4.2(8).</i>
Compression for DTLS and TLS	<p>To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients.</p> <p><b>Note</b> Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced.</p> <p>We introduced or modified the following commands: <b>anyconnect dtls compression [lzs   none]</b> and <b>anyconnect ssl compression [deflate   lzs   none]</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Group Policies &gt; Edit &gt; Edit Internal Group Policy &gt; Advanced &gt; AnyConnect Client &gt; SSL Compression.</p> <p><i>Also available in Version 8.2(5.13) and 8.4.2(8).</i></p>

**Table 22**      ***New Features for ASA Interim Version 8.3(2.25)/ASDM Version 6.4(5.106) (continued)***

Feature	Description
<b>Troubleshooting Features</b>	
Regular expression matching for the <b>show asp table classifier</b> and <b>show asp table filter</b> commands	<p>You can now enter the <b>show asp table classifier</b> and <b>show asp table filter</b> commands with a regular expression to filter output.</p> <p>We modified the following commands: <b>show asp table classifier match <i>regex</i></b>, <b>show asp table filter match <i>regex</i></b>.</p> <p>ASDM does not support this command; enter the command using the Command Line Tool.</p> <p><i>Also available in Version 8.2(5.13) and 8.4.2(8).</i></p>

## New Features in ASA 8.3(2)/ASDM 6.3(2)

Released: August 2, 2010

[Table 12](#) lists the new features for ASA Version 8.3(2)/ASDM Version 6.3(2).

**Table 23**      ***New Features for ASA Version 8.3(2)/ASDM Version 6.3(2)***

Feature	Description
<b>Monitoring Features</b>	
Enhanced logging and connection blocking	<p>When you configure a syslog server to use TCP, and the syslog server is unavailable, the ASA blocks new connections that generate syslog messages until the server becomes available again (for example, VPN, firewall, and cut-through-proxy connections). This feature has been enhanced to also block new connections when the logging queue on the ASA is full; connections resume when the logging queue is cleared.</p> <p>This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommend allowing new connections when syslog messages cannot be sent. To allow new connections, configure the syslog server to use UDP or use the <b>logging permit-hostdown</b> command check the <b>Allow user traffic to pass when TCP syslog server is down</b> check box on the Configuration &gt; Device Management &gt; Logging &gt; Syslog Servers pane.</p> <p>The following commands were modified: <b>show logging</b>.</p> <p>The following syslog messages were introduced: 414005, 414006, 414007, and 414008</p> <p>No ASDM screens were modified.</p>
Syslog message filtering and sorting	<p>Support has been added for the following:</p> <ul style="list-style-type: none"> <li>Syslog message filtering based on multiple text strings that correspond to various columns</li> <li>Creation of custom filters</li> <li>Column sorting of messages. For detailed information, see the <i>Cisco ASA 5500 Series Configuration Guide using ASDM</i>.</li> </ul> <p>The following screens were modified:</p> <p>Monitoring &gt; Logging &gt; Real-Time Log Viewer &gt; View</p> <p>Monitoring &gt; Logging &gt; Log Buffer Viewer &gt; View</p> <p><i>This feature interoperates with all ASA versions.</i></p>

**Table 23**      **New Features for ASA Version 8.3(2)/ASDM Version 6.3(2) (continued)**

Feature	Description
Clearing syslog messages for the CSC SSM	Support for clearing syslog messages has been added in the Latest CSC Security Events pane. The following screen was modified: Home > Content Security. <i>This feature interoperates with all ASA versions.</i>
<b>Remote Access Features</b>	
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	<p>(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware.</p> <p><b>Note</b> For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment.</p> <p>The following commands were introduced or modified: <b>crypto engine large-mod-accel</b>, <b>clear configure crypto engine</b>, <b>show running-config crypto engine</b>, and <b>show running-config crypto</b>.</p> <p>In ASDM, use the Command Line Interface tool to enter the <b>crypto engine large-mod-accel</b> command.</p> <p><i>Also available in Version 8.2(3).</i></p>
Microsoft Internet Explorer proxy lockdown control	<p>Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged; the default setting for the tab can be shown or hidden, depending on the user registry settings.</p> <p>The following command was introduced: <b>msie-proxy lockdown</b>.</p> <p>In ASDM, use the Command Line Interface tool to enter this command.</p> <p><i>Also available in Version 8.2(3).</i></p>
Secondary password enhancement	<p>You can now configure SSL VPN support for a common secondary password for all authentications or use the primary password as the secondary password.</p> <p>The following command was modified: <b>secondary-pre-fill-username [use-primary-password   use-common-password] ]</b></p> <p>The following screen was modified: Configuration &gt; Remote Access VPN &gt; Clientless SSL Access &gt; Connection Profiles &gt; Add/Edit Clientless SSL VPN Connection Profile &gt; Advanced &gt; Secondary Authentication.</p>

**Table 23**      ***New Features for ASA Version 8.3(2)/ASDM Version 6.3(2) (continued)***

Feature	Description
<b>General Features</b>	
No Payload Encryption image for export	<p>For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. For version 8.3(2), you can now install a No Payload Encryption image (asa832-npe-k8.bin) on the following models:</p> <ul style="list-style-type: none"> <li>• ASA 5505</li> <li>• ASA 5510</li> <li>• ASA 5520</li> <li>• ASA 5540</li> <li>• ASA 5550</li> </ul> <p>Features that are disabled in the No Payload Encryption image include:</p> <ul style="list-style-type: none"> <li>• Unified Communications.</li> <li>• Strong encryption for VPN (DES encryption is still available for VPN).</li> <li>• VPN load balancing (note that the CLI GUI is still present; the feature will not function, however).</li> <li>• Downloading of the dynamic database for the Botnet Traffic Filer (Static black and whitelists are still supported. Note that the CLI GUI is still present; the feature will not function, however.).</li> <li>• Management protocols requiring strong encryption, including SSL, SSHv2, and SNMPv3. You can, however, use SSL or SNMPv3 using base encryption (DES). Also, SSHv1 and SNMPv1 and v2 are still available.</li> </ul> <p>If you attempt to install a Strong Encryption (3DES/AES) license, you see the following warning:</p> <pre>WARNING: Strong encryption types have been disabled in this image; the VPN-3DES-AES license option has been ignored.</pre>

## New Features in ASA 8.3(1)/ASDM 6.3(1)

Released: March 8, 2010




Table 21 lists the new features for ASA Version 8.3(1)/ASDM Version 6.3(1).

**Table 24**      **New Features for ASA Version 8.3(1)/ASDM Version 6.3(1)**

Feature	Description
<b>Remote Access Features</b>	
Smart Tunnel Enhancements	<p>Logoff enhancement—Smart tunnel can now be logged off when all browser windows have been closed (parent affinity), or you can right click the notification icon in the system tray and confirm log out.</p> <p>Tunnel Policy—An administrator can dictate which connections go through the VPN gateway and which do not. An end user can browse the Internet directly while accessing company internal resources with smart tunnel if the administrator chooses.</p> <p>Simplified configuration of which applications to tunnel—When a smart tunnel is required, a user no longer needs to configure a list of processes that can access smart tunnel and in turn access certain web pages. An “enable smart tunnel” check box for either a bookmark or standalone application allows for an easier configuration process.</p> <p>Group policy home page—Using a check box in ASDM, administrators can now specify their home page in group policy in order to connect via smart tunnel.</p> <p>The following commands were introduced: <b>smart-tunnel network</b>, <b>smart-tunnel tunnel-policy</b>.</p> <p>The following screen was modified: Configuration &gt; Remote Access VPN &gt; AAA/Local Users &gt; Local Users &gt; Edit &gt; VPN Policy &gt; Clientless SSL VPN.</p>
Newly Supported Platforms for Browser-based VPN	<p>Release 8.3(1) provides browser-based (clientless) VPN access from the following newly supported platforms:</p> <ul style="list-style-type: none"> <li>Windows 7 x86 (32-bit) and x64 (64-bit) via Internet Explorer 8.x and Firefox 3.x</li> <li>Windows Vista x64 via Internet Explorer 7.x/8.x, or Firefox 3.x.</li> <li>Windows XP x64 via Internet Explorer 6.x/7.x/8.x and Firefox 3.x</li> <li>Mac OS 10.6.x 32- and 64-bit via Safari 4.x and Firefox 3.x.</li> </ul> <p>Firefox 2.x is likely to work, although we no longer test it.</p> <p>Release 8.3(1) introduces browser-based support for 64-bit applications on Mac OS 10.5.</p> <p>Release 8.3(1) now supports smart tunnel access on all 32-bit and 64-bit Windows OSs supported for browser-based VPN access, Mac OS 10.5 running on an Intel processor only, and Mac OS 10.6.x. The ASA does not support port forwarding on 64-bit OSs.</p> <p>Browser-based VPN access does not support Web Folders on Windows 7, Vista, and Internet Explorer 8.</p> <p>An ActiveX version of the RDP plug-in is not available for 64-bit browsers.</p> <p><b>Note</b> Windows 2000 and Mac OS X 10.4 are no longer supported for browser-based access.</p>

**Table 24**      **New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)**

Feature	Description
IPv6 support for IKEv1 LAN-to-LAN VPN connections	<p>For LAN-to-LAN connections using mixed IPv4 and IPv6 addressing, or all IPv6 addressing, the ASA supports VPN tunnels if both peers are Cisco ASA 5500 series ASAs, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6).</p> <p>Specifically, the following topologies are supported when both peers are Cisco ASA 5500 series ASAs:</p> <ul style="list-style-type: none"> <li>• The ASAs have IPv4 inside networks and the outside network is IPv6 (IPv4 addresses on the inside interfaces and IPv6 addresses on the outside interfaces).</li> <li>• The ASAs have IPv6 inside networks and the outside network is IPv4 (IPv6 addresses on the inside interface and IPv4 addresses on the outside interfaces).</li> <li>• The ASAs have IPv6 inside networks and the outside network is IPv6 (IPv6 addresses on the inside and outside interfaces).</li> </ul> <p> <b>Note</b> The defect CSCtd38078 currently prevents the Cisco ASA 5500 series from connecting to a Cisco IOS device as the peer device of a LAN-to-LAN connection.</p> <p>The following commands were modified or introduced: <b>isakmp enable</b>, <b>crypto map</b>, <b>crypto dynamic-map</b>, <b>tunnel-group</b>, <b>ipv6-vpn-filter</b>, <b>vpn-sessiondb</b>, <b>show crypto isakmp sa</b>, <b>show crypto ipsec sa</b>, <b>show crypto debug-condition</b>, <b>show debug crypto</b>, <b>show vpn-sessiondb</b>, <b>debug crypto condition</b>, <b>debug menu ike</b>.</p> <p>The following screens were modified or introduced:</p> <p>Wizards &gt; IPsec VPN Wizard, Configuration &gt; Site-to-Site VPN &gt; Connection Profiles  Configuration &gt; Site-to-Site VPN &gt; Connection Profiles &gt; Basic &gt; Add IPsec Site-to-Site Connection Profile  Configuration &gt; Site-to-Site VPN &gt; Group Policies  Configuration &gt; Site-to-Site VPN &gt; Group Policies &gt; Edit Internal Group Policy  Configuration &gt; Site-to-Site VPN &gt; Advanced &gt; Crypto Maps  Configuration &gt; Site-to-Site VPN &gt; Advanced &gt; Crypto Maps &gt; Add &gt; Create IPsec Rule  Configuration &gt; Site-to-Site VPN &gt; Advanced &gt; ACL Manager</p>
Plug-in for AnyConnect Profile Editor	<p>The AnyConnect Profile Editor is a convenient GUI-based configuration tool you can use to configure the AnyConnect 2.5 or later client profile, an XML file containing settings that control client features. Previously, you could only change profile settings manually by editing the XML tags in the profile file. The AnyConnect Profile Editor is a plug-in binary file named anyconnectprof.sgz packaged with the ASDM image and installed in the root directory of disk0:/ in the flash memory on the ASA. This design allows you to update the editor to be compatible with new AnyConnect features available in new client releases.</p>
SSL VPN Portal Customization Editor	<p>You can rebrand and customize the screens presented to clientless SSL VPN users using the new Edit Customization Object window in ASDM. You can customize the login, portal and logout screens, including corporate logos, text messages, and the general layout. Previously, the customization feature was embedded in the ASA software image. Moving it to ASDM provides greater usability for this feature and future enhancements.</p> <p>The following screen was modified: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Customization.</p>

**Table 24**      **New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)**

Feature	Description
Usability Improvements for Remote Access VPN	<p>ASDM provides a step-by-step guide to configuring Clientless SSL VPN, AnyConnect SSL VPN Remote Access, or IPsec Remote Access using the ASDM Assistant. The ASDM Assistant is more comprehensive than the VPN wizards, which are designed only to get you up and running.</p> <p>The following screen was modified: Configuration &gt; Remote Access VPN &gt; Introduction &gt; ASDM Assistant.</p>
<b>Firewall Features</b>	
Interface-Independent Access Policies	<p>You can now configure access rules that are applied globally, as well as access rules that are applied to an interface. If the configuration specifies both a global access policy and interface-specific access policies, the interface-specific policies are evaluated before the global policy.</p> <p>The following command was modified: <b>access-group global</b>.</p> <p>The following screen was modified: Configuration &gt; Firewall &gt; Access Rules.</p>
Network and Service Objects	<p>You can now create named network objects that you can use in place of a host, a subnet, or a range of IP addresses in your configuration and named service objects that you can use in place of a protocol and port in your configuration. You can then change the object definition in one place, without having to change any other part of your configuration. This release introduces support for network and service objects in the following features:</p> <ul style="list-style-type: none"> <li>• NAT</li> <li>• Access lists rules</li> <li>• Network object groups</li> </ul> <p><b>Note</b> ASDM used network objects internally in previous releases; this feature introduces platform support for network objects.</p> <p>The following commands were introduced or modified: <b>object network</b>, <b>object service</b>, <b>show running-config object</b>, <b>clear configure object</b>, <b>access-list extended</b>, <b>object-group network</b>.</p> <p>The following screens were modified or introduced:  Configuration &gt; Firewall &gt; Objects &gt; Network Objects/Groups, Configuration &gt; Firewall &gt; Objects &gt; Service Objects/Groups  Configuration &gt; Firewall &gt; NAT Rules, Configuration &gt; Firewall &gt; Access Rules</p>
Object-group Expansion Rule Reduction	<p>Significantly reduces the network object-group expansion while maintaining a satisfactory level of packet classification performance.</p> <p>The following commands were modified: <b>show object-group</b>, <b>clear object-group</b>, <b>show access-list</b>.</p> <p>The following screen was modified: Configuration &gt; Firewall &gt; Access Rules &gt; Advanced.</p>

**Table 24**      ***New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)***

Feature	Description
NAT Simplification	<p>The NAT configuration was completely redesigned to allow greater flexibility and ease of use. You can now configure NAT using auto NAT, where you configure NAT as part of the attributes of a network object, and manual NAT, where you can configure more advanced NAT options.</p> <p>The following commands were introduced or modified: <b>nat</b> (in global and object network configuration mode), <b>show nat</b>, <b>show nat pool</b>, <b>show xlate</b>, <b>show running-config nat</b>.</p> <p>The following commands were removed: <b>global</b>, <b>static</b>, <b>nat-control</b>, <b>alias</b>.</p> <p>The following screens were modified or introduced:</p> <p>Configuration &gt; Firewall &gt; Objects &gt; Network Objects/Group</p> <p>Configuration &gt; Firewall &gt; NAT Rules</p>
Use of Real IP addresses in access lists instead of translated addresses	<p>When using NAT, mapped addresses are no longer required in an access list for many features. You should always use the real, untranslated addresses when configuring these features. Using the real address means that if the NAT configuration changes, you do not need to change the access lists.</p> <p>The following commands and features that use access lists now use real IP addresses. These features are automatically migrated to use real IP addresses when you upgrade to 8.3, unless otherwise noted.</p> <ul style="list-style-type: none"> <li>• <b>access-group</b> command Access rules</li> <li>• Modular Policy Framework <b>match access-list</b> command Service policy rules</li> <li>• Botnet Traffic Filter <b>dynamic-filter enable classify-list</b> command</li> <li>• AAA <b>aaa ... match</b> commands rules</li> <li>• WCCP <b>wccp redirect-list group-list</b> command redirect.</li> </ul> <p><b>Note</b> WCCP is not automatically migrated when you upgrade to 8.3.</p>
Threat Detection Enhancements	<p>You can now customize the number of rate intervals for which advanced statistics are collected. The default number of rates was changed from 3 to 1. For basic statistics, advanced statistics, and scanning threat detection, the memory usage was improved.</p> <p>The following commands were modified: <b>threat-detection statistics port number-of-rates</b>, <b>threat-detection statistics protocol number-of-rates</b>, <b>show threat-detection memory</b>.</p> <p>The following screen was modified: Configuration &gt; Firewall &gt; Threat Detection.</p>
<b>Unified Communication Features</b>	
SCCP v19 support	<p>The IP phone support in the Cisco Phone Proxy feature was enhanced to include support for version 19 of the SCCP protocol on the list of supported IP phones.</p>

**Table 24**      **New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)**

Feature	Description
Cisco Intercompany Media Engine Proxy	<p>Cisco Intercompany Media Engine (UC-IME) enables companies to interconnect on-demand, over the Internet with advanced features made available by VoIP technologies. Cisco Intercompany Media Engine allows for business-to-business federation between Cisco Unified Communications Manager clusters in different enterprises by utilizing peer-to-peer, security, and SIP protocols to create dynamic SIP trunks between businesses. A collection of enterprises work together to end up looking like one large business with inter-cluster trunks between them.</p> <p>The following commands were modified or introduced: <b>uc-ime</b>, <b>fallback hold-down</b>, <b>fallback monitoring</b>, <b>fallback sensitivity-file</b>, <b>mapping-service listening-interface</b>, <b>media-termination</b>, <b>ticket epoch</b>, <b>ucm address</b>, <b>clear configure uc-ime</b>, <b>debug uc-ime</b>, <b>show running-config uc-ime</b>, <b>inspect sip</b>.</p> <p>The following screens were modified or introduced:</p> <p>Wizards &gt; Unified Communications Wizard &gt; Cisco Intercompany Media Engine Proxy Configuration &gt; Firewall &gt; Unified Communications, and then click UC-IME Proxy Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; Select SIP Inspection Map</p>
SIP Inspection Support for IME	<p>SIP inspection has been enhance to support the new Cisco Intercompany Media Engine (UC-IME) Proxy.</p> <p>The following command was modified: <b>inspect sip</b>.</p> <p>The following screen was modified: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; Select SIP Inspection Map.</p>
Unified Communication Wizard	<p>The Unified Communications wizard guides you through the complete configuration and automatically configures required aspects for the following proxies: Cisco Mobility Advantage Proxy, Cisco Presence Federation Proxy, Cisco Intercompany Media Engine proxy. Additionally, the Unified Communications wizard automatically configures other required aspects of the proxies.</p> <p>The following screens were modified:</p> <p>Wizards &gt; Unified Communications Wizard Configuration &gt; Firewall &gt; Unified Communications</p>
Enhanced Navigation for Unified Communication Features	<p>The Unified Communications proxy features, such as the Phone Proxy, TLS Proxy, CTL File, and CTL Provider pages, are moved from under the Objects category in the left Navigation panel. to the new Unified Communications category. In addition, this new category contains pages for the new Unified Communications wizard and the UC-IME Proxy page.</p> <p><i>This feature interoperates with all ASA versions.</i></p>
<b>Routing Features</b>	
Route map support	<p>ASDM has added enhanced support for static and dynamic routes.</p> <p>The following screen was modified: Configuration &gt; Device Setup &gt; Routing &gt; Route Maps.</p> <p><i>This feature interoperates with all ASA versions.</i></p>
<b>Monitoring Features</b>	
Time Stamps for Access List Hit Counts	<p>Displays the timestamp, along with the hash value and hit count, for a specified access list.</p> <p>The following command was modified: <b>show access-list</b>.</p> <p>The following screen was modified: Configuration &gt; Firewall &gt; Access Rules. (The timestamp appears when you hover the mouse over a cell in the Hits column.)</p>

**Table 24**      ***New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)***

<b>Feature</b>	<b>Description</b>
High Performance Monitoring for ASDM	<p>You can now enable high performance monitoring for ASDM to show the top 200 hosts connected through the ASA. Each entry of a host contains the IP address of the host and the number of connections initiated by the host, and is updated every 120 seconds.</p> <p>The following commands were introduced: <b>hpm topn enable</b>, <b>clear configure hpm</b>, <b>show running-config hpm</b>.</p> <p>The following screen was introduced: Home &gt; Firewall Dashboard &gt; Top 200 Hosts.</p>
<b>Licensing Features</b>	
Non-identical failover licenses	<p>Failover licenses no longer need to be identical on each unit. The license used for both units is the combined license from the primary and secondary units.</p> <p><b>Note</b> For the ASA 5505 and 5510 ASAs, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license.</p> <p>The following commands were modified: <b>show activation-key</b> and <b>show version</b>.</p> <p>The following screen was modified: Configuration &gt; Device Management &gt; Licensing &gt; Activation Key.</p>
Stackable time-based licenses	<p>Time-based licenses are now stackable. In many cases, you might need to renew your time-based license and have a seamless transition from the old license to the new one. For features that are only available with a time-based license, it is especially important that the license not expire before you can apply the new license. The ASA allows you to <i>stack</i> time-based licenses so you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early. For licenses with numerical tiers, stacking is only supported for licenses with the same capacity, for example, two 1000-session SSL VPN licenses. You can view the state of the licenses using the show activation-key command at Configuration &gt; Device Management &gt; Licensing &gt; Activation Key.</p>
Intercompany Media Engine License	<p>The IME license was introduced.</p>
Multiple time-based licenses active at the same time	<p>You can now install multiple time-based licenses, and have one license per feature active at a time.</p> <p>The following commands were modified: <b>show activation-key</b> and <b>show version</b>.</p> <p>The following screen was modified: Configuration &gt; Device Management &gt; Licensing &gt; Activation Key.</p>
Discrete activation and deactivation of time-based licenses.	<p>You can now activate or deactivate time-based licenses using a command.</p> <p>The following command was modified: <b>activation-key [activate   deactivate]</b>.</p> <p>The following screen was modified: Configuration &gt; Device Management &gt; Licensing &gt; Activation Key.</p>
<b>General Features</b>	

**Table 24**      **New Features for ASA Version 8.3(1)/ASDM Version 6.3(1) (continued)**

Feature	Description
Master Passphrase	<p>The master passphrase feature allows you to securely store plain text passwords in encrypted format. It provides a master key that is used to universally encrypt or mask all passwords, without changing any functionality. The Backup/Restore feature supports the master passphrase.</p> <p>The following commands were introduced: <b>key config-key password-encryption, password encryption aes.</b></p> <p>The following screens were introduced:</p> <p>Configuration &gt; Device Management &gt; Advanced &gt; Master Passphrase  Configuration &gt; Device Management &gt; Device Administration &gt; Master Passphrase</p>
<b>ASDM Features</b>	
Upgrade Software from Cisco.com Wizard	<p>The Upgrade Software from Cisco.com wizard has changed to allow you to automatically upgrade ASDM and the ASA to more current versions. Note that this feature is only available in single mode and, in multiple context mode, in the System execution space. It is not available in a context.</p> <p>The following screen was modified: Tools &gt; Check for ASA/ASDM Updates.</p> <p><i>This feature interoperates with all ASA versions.</i></p>
Backup/Restore Enhancements	<p>The Backup Configurations pane was re-ordered and re-grouped so you can choose the files you want to backup more easily. A Backup Progress pane was added allowing you to visually measure the progress of the backup. And you will see significant performance improvement when using backup or restore.</p> <p>The following screen was modified: Tools &gt; Backup Configurations or Tools &gt; Restore Configurations.</p> <p><i>This feature interoperates with all ASA versions.</i></p>

## New Features in Version 8.2

This section includes the following topics:

- [New Features in ASA 8.2\(5.13\)/ASDM 6.4\(4.106\), page 81](#)
- [New Features in ASA 8.2\(5\)/ASDM 6.4\(3\), page 82](#)
- [New Features in ASA 8.2\(4.4\)/ASDM 6.3\(5\), page 85](#)
- [New Features in ASA 8.2\(4.1\)/ASDM 6.3\(5\), page 86](#)
- [New Features in ASA 8.2\(4\)/ASDM 6.3\(5\), page 86](#)
- [New Features in ASA 8.2\(3.9\)/ASDM 6.3\(4\), page 87](#)
- [New Features in ASA 8.2\(3\)/ASDM 6.3\(3\) and 6.3\(4\), page 87](#)
- [New Features in ASA 8.2\(2\)/ASDM 6.2\(5\), page 89](#)
- [New Features in ASA 8.2\(1\)/ASDM 6.2\(1\), page 91](#)

## New Features in ASA 8.2(5.13)/ASDM 6.4(4.106)

**Released: September 18, 2011**

Table 18 lists the new features for ASA interim Version 8.2(5.13)/ASDM Version 6.4(5.106).



### Note

We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

**Table 25**      **New Features for ASA Interim Version 8.2(5.13)/ASDM Version 6.4(5.106)**

Feature	Description
<b>Remote Access Features</b>	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. <i>Also available in Version 8.3(2.25) and 8.4.2(8).</i>
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients.  <b>Note</b> Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced.  We introduced or modified the following commands: <b>anyconnect dtls compression [lzs   none]</b> and <b>anyconnect ssl compression [deflate   lzs   none]</b> .  We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy > Advanced > AnyConnect Client > SSL Compression.  <i>Also available in Version 8.3(2.25) and Version 8.4.2(8).</i>
<b>Troubleshooting Features</b>	
Regular expression matching for the <b>show asp table classifier</b> and <b>show asp table filter</b> commands	You can now enter the <b>show asp table classifier</b> and <b>show asp table filter</b> commands with a regular expression to filter output.  We modified the following commands: <b>show asp table classifier match regex</b> , <b>show asp table filter match regex</b> .  ASDM does not support this command; enter the command using the Command Line Tool.  <i>Also available in Version 8.3(2.25) and Version 8.4.2(8).</i>



## New Features in ASA 8.2(5)/ASDM 6.4(3)

Released: May 23, 2011

Table 26 lists the new features for ASA Version 8.2(5)/ASDM Version 6.4(3).

**Table 26**      **New Features for ASA Version 8.2(5)/ASDM Version 6.4(3)**

Feature	Description
<b>Monitoring Features</b>	
Smart Call-Home Anonymous Reporting	<p>Customers can now help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device.</p> <p>We introduced the following commands: <b>call-home reporting anonymous</b>, <b>call-home test reporting anonymous</b>.</p> <p>We modified the following screen: Configuration &gt; Device Monitoring &gt; Smart Call-Home.</p> <p><i>Also available in Version 8.4(2).</i></p>
IF-MIB ifAlias OID support	<p>The ASA now supports the ifAlias OID. When you browse the IF-MIB, the ifAlias OID will be set to the value that has been set for the interface description.</p> <p><i>Also available in Version 8.4(2).</i></p>
<b>Remote Access Features</b>	
Portal Access Rules	<p>This enhancement allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in the HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources.</p> <p>We modified the following command: <b>portal-access-rule</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Portal Access Rules.</p> <p><i>Also available in Version 8.4(2).</i></p>

**Table 26**      ***New Features for ASA Version 8.2(5)/ASDM Version 6.4(3) (continued)***

Feature	Description
Mobile Posture (formerly referred to as AnyConnect Identification Extensions for Mobile Device Detection)	<p>You can now configure the ASA to permit or deny VPN connections to mobile devices, enable or disable mobile device access on a per-group basis, and gather information about connected mobile devices based on the mobile device posture data. The following mobile platforms support this capability: AnyConnect for iPhone/iPad/iPod Versions 2.5.x and AnyConnect for Android Version 2.4.x. You do not need to enable CSD to configure these attributes in ASDM.</p> <p><b>Licensing Requirements</b></p> <p>Enforcing remote access controls and gathering posture data from mobile devices requires an AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to be installed on the ASA. You receive the following functionality based on the license you install:</p> <ul style="list-style-type: none"> <li>• <b>AnyConnect Premium License Functionality</b> Enterprises that install the AnyConnect Premium license will be able to enforce DAP policies, on supported mobile devices, based on these DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device.</li> <li>• <b>AnyConnect Essentials License Functionality</b> Enterprises that install the AnyConnect Essentials license will be able to do the following: <ul style="list-style-type: none"> <li>– Enable or disable mobile device access on a per-group basis and to configure that feature using ASDM.</li> <li>– Display information about connected mobile devices via CLI or ASDM without having the ability to enforce DAP policies or deny or allow remote access to those mobile devices.</li> </ul> </li> </ul> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Dynamic Access Policies &gt; Add/Edit Endpoint Attributes &gt; Endpoint Attribute Type:AnyConnect.</p> <p><i>Also available in Version 8.4(2).</i></p>
Split Tunnel DNS policy for AnyConnect	<p>This release includes a new policy pushed down to the AnyConnect Secure Mobility Client for resolving DNS addresses over split tunnels. This policy applies to VPN connections using the SSL or IPsec/IKEv2 protocol and instructs the AnyConnect client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyConnect client does not try to resolve the address through public DNS servers.</p> <p>By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy—tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list.</p> <p>We introduced the following command: <b>split-tunnel-all-dns</b>.</p> <p>We modified the following screen: Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; Add/Edit Group Policy &gt; Advanced &gt; Split Tunneling (see the Send All DNS Lookups Through Tunnel check box).</p> <p><i>Also available in Version 8.4(2).</i></p>

**Table 26**      **New Features for ASA Version 8.2(5)/ASDM Version 6.4(3) (continued)**

Feature	Description
SSL SHA-2 digital signature	<p>You can now use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5(1) or later (2.5(2) or later recommended). This release does not support SHA-2 for other uses or products.</p> <p>Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image.</p> <p>We modified the following command: <b>show crypto ca certificate</b> (the Signature Algorithm field identifies the digest algorithm used when generating the signature).</p> <p>We did not modify any screens.</p> <p><i>Also available in Version 8.4(2).</i></p>
L2TP/IPsec support for Android	<p>We now support VPN connections between Android mobile devices and ASA 5500 series devices, when using the L2TP/IPsec protocol and the native Android VPN client. Mobile devices must be using the Android 2.1 or later operating system.</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p> <p><i>Also available in Version 8.4(1).</i></p>
SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients	<p>ASA supports SHA2 certificate signature support for Microsoft Windows 7 and Android-native VPN clients when using the L2TP/IPsec protocol.</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p> <p><i>Also available in Version 8.4(2).</i></p>
Enable/disable certificate mapping to override the group-url attribute	<p>This feature changes the preference of a connection profile during the connection profile selection process. By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This optional feature changes the preference to a connection profile that specifies the group URL requested by the endpoint. The new option lets administrators rely on the group URL preference used by many older ASA software releases.</p> <p>We introduced the following command: <b>tunnel-group-preference</b>.</p> <p>We modified the following screens:</p> <p>Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN &gt; Connection Profiles  Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles</p> <p><i>Also available in Version 8.4(2).</i></p>

**Interface Features**

**Table 26**      **New Features for ASA Version 8.2(5)/ASDM Version 6.4(3) (continued)**

Feature	Description
Support for Pause Frames for Flow Control on 1-Gigabit Ethernet Interface	<p>You can now enable pause (XOFF) frames for flow control on 1-Gigabit Ethernet interfaces; support was previously added for 10-Gigabit Ethernet interfaces in 8.2(2).</p> <p>We modified the following command: <b>flowcontrol</b>.</p> <p>We modified the following screens:</p> <p>(Single Mode) Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface &gt; General  (Multiple Mode, System) Configuration &gt; Interfaces &gt; Add/Edit Interface</p> <p><i>Also available in Version 8.4(2).</i></p>
<b>Unified Communications Features</b>	
ASA-Tandberg Interoperability with H.323 Inspection	<p>H.323 Inspection now supports uni-directional signaling for two-way video sessions. This enhancement allows H.323 Inspection of one-way video conferences supported by Tandberg video phones. Supporting uni-directional signaling allows Tandberg phones to switch video modes (close their side of an H.263 video session and reopen the session using H.264, the compression standard for high-definition video).</p> <p>We did not modify any commands.</p> <p>We did not modify any screens.</p> <p><i>Also available in Version 8.4(2).</i></p>
<b>Routing Features</b>	
Timeout for connections using a backup static route	<p>When multiple static routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value.</p> <p>We modified the following command: <b>timeout floating-conn</b>.</p> <p>We modified the following screen: Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</p> <p><i>Also available in Version 8.4(2).</i></p>

## New Features in ASA 8.2(4.4)/ASDM 6.3(5)

**Released: March 4, 2011**

**Released: March 4, 2011**

[Table 27](#) lists the new features for ASA Version 8.2(4.4)/ASDM Version 6.3(5).



### Note

We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

**Table 27**      **New Features for ASA Version 8.2(4.4)/ASDM Version 6.3(5)**

Feature	Description
<b>Hardware Features</b>	
Support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X	We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10.
<b>Remote Access Features</b>	
Clientless SSL VPN support for Outlook Web Access 2010	By default, Clientless SSL VPN now provides content transformation (rewriting) support for Outlook Web Access (OWA) 2010 traffic.  We did not modify any commands.  We did not modify any screens.

## New Features in ASA 8.2(4.1)/ASDM 6.3(5)

**Released: January 18, 2011**

Table 28 lists the new features for ASA Version 8.2(4.1)/ASDM Version 6.3(5).



### Note

We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

**Table 28**      **New Features for ASA Version 8.2(4.1)/ASDM Version 6.3(5)**

Feature	Description
<b>Remote Access Features</b>	
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommended). This release does not support SHA-2 for other uses or products. This feature does not involve configuration changes. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. To support this feature, we added the Signature Algorithm field to the <b>show crypto ca certificate</b> command to identify the digest algorithm used when generating the signature.

## New Features in ASA 8.2(4)/ASDM 6.3(5)

Released: December 15, 2010

Table 29 lists the new features for ASA Version 8.2(4)/ASDM Version 6.3(5).

**Table 29**      **New Features for ASA Version 8.2(4)/ASDM Version 6.3(5)**

Feature	Description
<b>Hardware Features</b>	
Support for the Cisco ASA 5585-X with SSP-10 and SSP-40	We introduced support for the ASA 5585-X with Security Services Processor (SSP)-10 and -40. <b>Note</b> The ASA 5585-X is not supported in Version 8.3(x).

## New Features in ASA 8.2(3.9)/ASDM 6.3(4)

Released: November 2, 2010

Table 30 lists the new features for ASA interim Version 8.2(3.9)/ASDM Version 6.3(4).



**Note**

We recommend that you upgrade to a Cisco.com-posted interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available. We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each interim release, see the *Cisco ASA Interim Release Notes* available on the Cisco.com software download site.

**Table 30**      **New Features for ASA Version 8.2(3.9)/ASDM Version 6.3(4)**

Feature	Description
<b>Remote Access Features</b>	
SSL SHA-2 digital signature	This release supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates. Our support for SHA-2 includes all three hash sizes: SHA-256, SHA-384, and SHA-512. SHA-2 requires AnyConnect 2.5.1 or later (2.5.2 or later recommended). This release does not support SHA-2 for other uses or products. This feature does not involve configuration changes. Caution: To support failover of SHA-2 connections, the standby ASA must be running the same image. To support this feature, we added the Signature Algorithm field to the <b>show crypto ca certificate</b> command to identify the digest algorithm used when generating the signature.

## New Features in ASA 8.2(3)/ASDM 6.3(3) and 6.3(4)

Released: August 9, 2010

Table 31 Table 31 lists the new features for ASA Version 8.2(3)/ASDM Version 6.3(3)/6.3(4).



**Note**

ASDM 6.3(4) does not include any new features; it includes a caveat fix required for support of the ASA 5585-X.

**Table 31**      **New Features for ASA Version 8.2(3)/ASDM Version 6.3(3) and 6.3(4)**

Feature	Description
<b>Hardware Features</b>	
Support for the Cisco ASA 5585-X with SSP-20 and SSP-60	<p>Support for the ASA 5585-X with Security Services Processor (SSP)-20 and -60 was introduced.</p> <p><b>Note</b>    The ASA 5585-X is not supported in Version 8.3(x).</p> <p>             The ASA 5585-X requires ASDM 6.3(4).</p>
<b>Remote Access Features</b>	
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	<p>(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware.</p> <p><b>Note</b>    For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment.</p> <p><b>Note</b>    The ASA 5580/5585-X platforms already integrate this capability; therefore, crypto engine commands are not applicable on these platforms.</p> <p>The following commands were introduced or modified: <b>crypto engine large-mod-accel</b>, <b>clear configure crypto engine</b>, <b>show running-config crypto engine</b>, and <b>show running-config crypto</b>. In ASDM, use the Command Line Interface tool to enter the <b>crypto engine large-mod-accel</b> command.</p> <p><i>Also available in Version 8.3(2).</i></p>
Microsoft Internet Explorer proxy lockdown control	<p>Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged; the default setting for the tab can be shown or hidden, depending on the user registry settings.</p> <p>The following command was introduced: <b>msie-proxy lockdown</b>.</p> <p>In ASDM, use the Command Line Interface tool to enter this command.</p>
Trusted Network Detection Pause and Resume	<p>This feature enables the AnyConnect client to retain its session information and cookie so that it can seamlessly restore connectivity after the user leaves the office, as long as the session does not exceed the idle timer setting. This feature requires an AnyConnect release that supports TND pause and resume.</p>

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

Released: January 11, 2010

Table 32 lists the new features for ASA Version 8.2(2)/ASDM Version 6.2(5).

**Table 32**      **New Features for ASA Version 8.2(2)/ASDM Version 6.2(5)**

Feature	Description
<b>Remote Access Features</b>	
Scalable Solutions for Waiting-to-Resume VPN Sessions	<p>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.</p> <p>The following screen was modified: Monitoring &gt; VPN &gt; VPN Statistics &gt; Sessions.</p> <p><i>Also available in Version 8.0(5).</i></p>
<b>Application Inspection Features</b>	
Inspection for IP Options	<p>You can now control which IP packets with specific IP options should be allowed through the ASA. You can also clear IP options from an IP packet, and then allow it through the ASA. Previously, all IP options were denied by default, except for some special cases.</p> <p><b>Note</b> This inspection is enabled by default. The following command is added to the default global service policy: <b>inspect ip-options</b>. Therefore, the ASA allows RSVP traffic that contains packets with the Router Alert option (option 20) when the ASA is in routed mode.</p> <p>The following commands were introduced: <b>policy-map type inspect ip-options, inspect ip-options, eool, nop</b>.</p> <p>The following screens were introduced:</p> <p>Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; IP-Options  Configuration &gt; Firewall &gt; Service Policy &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; Protocol Inspection</p>
Enabling Call Set up Between H.323 Endpoints	<p>You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The ASA includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages.</p> <p>Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint IP address is unknown and the ASA opens a pinhole through source IP address/port 0/0. By default, this option is disabled.</p> <p>The following command was introduced: <b>ras-rcf-pinholes enable</b> (under the <b>policy-map type inspect h323 &gt; parameters</b> commands).</p> <p>The following screen was modified: Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; H.323 &gt; Details &gt; State Checking.</p> <p><i>Also available in Version 8.0(5).</i></p>
<b>Unified Communication Features</b>	
Mobility Proxy application no longer requires Unified Communications Proxy license	The Mobility Proxy no longer requires the UC Proxy license.
<b>Interface Features</b>	



**Table 32**      **New Features for ASA Version 8.2(2)/ASDM Version 6.2(5) (continued)**

Feature	Description
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	<p>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.</p> <p>The MAC addresses are also now persistent across reloads.</p> <p>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.</p> <p>The following command was modified: <b>mac-address auto prefix</b> <i>prefix</i>.</p> <p>The following screen was modified: Configuration &gt; Context Management &gt; Security Contexts.</p> <p><i>Also available in Version 8.0(5).</i></p>
Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces	<p>You can now enable pause (XOFF) frames for flow control.</p> <p>The following command was introduced: <b>flowcontrol</b>.</p> <p>The following screens were modified:</p> <p>(Single Mode) Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface &gt; General</p> <p>(Multiple Mode, System) Configuration &gt; Interfaces &gt; Add/Edit Interface</p>
<b>Firewall Features</b>	
Botnet Traffic Filter Enhancements	<p>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.</p> <p>The following commands were introduced or modified: <b>dynamic-filter ambiguous-is-black</b>, <b>dynamic-filter drop blacklist</b>, <b>show dynamic-filter statistics</b>, <b>show dynamic-filter reports infected-hosts</b>, and <b>show dynamic-filter reports top</b>.</p> <p>The following screens were introduced or modified:</p> <p>Configuration &gt; Firewall &gt; Botnet Traffic Filter &gt; Traffic Settings</p> <p>Monitoring &gt; Botnet Traffic Filter &gt; Infected Hosts</p>
Connection timeouts for all protocols	<p>The idle timeout was changed to apply to all protocols, not just TCP.</p> <p>The following command was modified: <b>set connection timeout</b>.</p> <p>The following screen was modified: Configuration &gt; Firewall &gt; Service Policies &gt; Rule Actions &gt; Connection Settings.</p>
<b>Routing Features</b>	
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	<p>This enhancement introduces ASA 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 ASA to send the Subnet Selection option or the Link Selection option.</p> <p>The following command was modified: <b>dhcp-server</b> [<b>subnet-selection</b>   <b>link-selection</b>].</p> <p>The following screen was modified: Remote Access VPN &gt; Network Access &gt; IPsec connection profiles &gt; Add/Edit.</p> <p><i>Also available in Version 8.0(5).</i></p>
<b>High Availability Features</b>	

**Table 32**      ***New Features for ASA Version 8.2(2)/ASDM Version 6.2(5) (continued)***

<b>Feature</b>	<b>Description</b>
IPv6 Support in Failover Configurations	<p>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.</p> <p>The following commands were modified: <b>failover interface ip, ipv6 address</b>.</p> <p>The following screens were modified:</p> <p>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</p>
No notifications when interfaces are brought up or brought down during a switchover event	<p>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.</p> <p><i>Also available in Version 8.0(5).</i></p>
<b>AAA Features</b>	
100 AAA Server Groups	<p>You can now configure up to 100 AAA server groups; the previous limit was 15 server groups.</p> <p>The following command was modified: <b>aaa-server</b>.</p> <p>The following screen was modified: Configuration &gt; Device Management &gt; Users/AAA &gt; AAA Server Groups.</p>
<b>Monitoring Features</b>	
Smart Call Home	<p>Smart Call Home offers proactive diagnostics and real-time alerts on the ASA 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.</p> <p><b>Note</b>    Smart Call Home server Version 3.0(1) has limited support for the ASA. See the “Important Notes” for more information.</p> <p>The following commands were introduced: <b>call-home, call-home send alert-group, call-home test, call-home send, service call-home, show call-home, show call-home registered-module status</b>.</p> <p>The following screen was introduced: Configuration&gt; Device Management&gt; Smart Call Home.</p>

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

Released: May 6, 2009

Table 33 lists the new features for ASA Version 8.2(1)/ASDM Version 6.2(1).

**Table 33**      **New Features for ASA Version 8.2(1)/ASDM Version 6.2(1)**

Feature	Description
<b>Remote Access Features</b>	
One Time Password Support for ASDM Authentication	<p>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.</p> <p>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.</p> <p>The following commands were introduced: <b>http server idle-timeout</b> and <b>http server session-timeout</b>. The <b>http server idle-timeout</b> default is 20 minutes, and can be increased up to a maximum of 1440 minutes.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; ASDM/HTTPD/Telnet/SSH.</p>
Customizing Secure Desktop	<p>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.</p> <p>In ASDM, see Configuration &gt; CSD Manager &gt; Secure Desktop Manager.</p>
Pre-fill Username from Certificate	<p>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. To use this feature, you must configure both the <b>pre-fill username</b> and the <b>username-from-certificate</b> commands in tunnel-group configuration mode.</p> <p>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. When configuring the pre-fill username feature for double authentication, the administrator uses the following new tunnel-group general-attributes configuration mode commands:</p> <ul style="list-style-type: none"> <li>• <b>secondary-pre-fill-username</b>—Enables username extraction for Clientless or AnyConnect client connection.</li> <li>• <b>secondary-username-from-certificate</b>—Allows for extraction of a few standard DN fields from a certificate for use as a username.</li> </ul> <p>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.</p>

**Table 33**      ***New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)***

Feature	Description
Double Authentication	<p>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.</p> <p>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.</p> <p>Double authentication requires the following new tunnel-group general-attributes configuration mode commands:</p> <ul style="list-style-type: none"> <li>• <b>secondary-authentication-server-group</b>—Specifies the secondary AAA server group, which cannot be an SDI server group.</li> <li>• <b>secondary-username-from-certificate</b>—Allows for extraction of a few standard DN fields from a certificate for use as a username.</li> <li>• <b>secondary-pre-fill-username</b>—Enables username extraction for Clientless or AnyConnect client connection.</li> <li>• <b>authentication-attr-from-server</b>—Specifies which authentication server authorization attributes are applied to the connection.</li> <li>• <b>authenticated-session-username</b>—Specifies which authentication username is associated with the session.</li> </ul> <p><b>Note</b>    The RSA/SDI authentication server type cannot be used as the secondary username/password credential. It can only be used for primary authentication.</p> <p>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.</p>

**Table 33**      **New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)**

Feature	Description
AnyConnect Essentials	<p>AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the ASA, that provides the full AnyConnect capability, with the following exceptions:</p> <ul style="list-style-type: none"> <li>• No CSD (including HostScan/Vault/Cache Cleaner)</li> <li>• No clientless SSL VPN</li> <li>• Optional Windows Mobile Support</li> </ul> <p>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.</p> <p>To configure AnyConnect Essentials, the administrator uses the following command:</p> <p><b>anyconnect-essentials</b>—Enables the AnyConnect Essentials feature. If this feature is disabled (using the <b>no</b> form of this command), the SSL Premium license is used. This feature is enabled by default.</p> <p><b>Note</b> This license cannot be used at the same time as the shared SSL VPN premium license.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; AnyConnect Essentials License. The AnyConnect Essentials license must be installed for ASDM to show this pane.</p>
Disabling Cisco Secure Desktop per Connection Profile	<p>When enabled, Cisco Secure Desktop automatically runs on all computers that make SSL VPN connections to the ASA. 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.</p> <p>CLI: <b>[no] without-csd command</b></p> <p><b>Note</b> “Connect Profile” in ASDM is also known as “Tunnel Group” in the CLI. Additionally, the <b>group-url</b> command is required for this feature. If the SSL VPN session uses connection-alias, this feature will not take effect.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Connection Profiles &gt; Add or Edit &gt; Advanced, Clientless SSL VPN Configuration.</p> <p>or</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles &gt; Add or Edit &gt; Advanced &gt; SSL VPN.</p>
Certificate Authentication Per Connection Profile	<p>Previous versions supported certificate authentication for each ASA 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; the <b>ssl certificate authentication</b> command is no longer needed, but the ASA retains it for backward compatibility.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles &gt; Add/Edit &gt; Basic.</p> <p>or</p> <p>Configuraiton &gt; Remote Access VPN &gt; Clientless SSL VPN &gt; Connection Profiles &gt; Add/Edit&gt;Basic.</p>

**Table 33**      ***New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
EKU Extensions for Certificate Mapping	<p>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.</p> <p>The following command was introduced: <b>extended-key-usage</b>.</p> <p>In ASDM, use the IPsec Certificate to Connection Maps &gt; Rules pane, or Certificate to SSL VPN Connections Profile Maps pane.</p>
SSL VPN SharePoint Support for Win 2007 Server	Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.
Shared license for SSL VPN sessions	<p>You can purchase a shared license with a large number of SSL VPN sessions and share the sessions as needed among a group of ASAs by configuring one of the ASAs as a shared license server, and the rest as clients. The following commands were introduced: <b>license-server</b> commands (various), <b>show shared license</b>.</p> <p><b>Note</b> This license cannot be used at the same time as the AnyConnect Essentials license.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Licensing &gt; Shared SSL VPN Licenses. Also see, Monitoring &gt; VPN &gt; Clientless SSL VPN &gt; Shared Licenses.</p>
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.
<b>Firewall Features</b>	
TCP state bypass	<p>If you have asymmetric routing configured on upstream routers, and traffic alternates between two ASAs, then you can configure TCP state bypass for specific traffic. The following command was introduced: <b>set connection advanced tcp-state-bypass</b>.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Rule Actions &gt; Connection Settings.</p>
Per-Interface IP Addresses for the Media-Termination Instance Used by the Phone Proxy	<p>In Version 8.0(4), you configured a global media-termination address (MTA) on the ASA. 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.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; Media Termination Address.</p>
Displaying the CTL File for the Phone Proxy	<p>The Cisco Phone Proxy feature includes the <b>show ctl-file</b> command, which shows the contents of the CTL file used by the phone proxy. Using the <b>show ctl-file</b> command is useful for debugging when configuring the phone proxy instance.</p> <p>This command is not supported in ASDM.</p>

**Table 33**      ***New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
Clearing Secure-phone Entries from the Phone Proxy Database	<p>The Cisco Phone Proxy feature includes the <b>clear phone-proxy secure-phones</b> command, which clears the secure-phone entries in the phone proxy database. Because secure IP phones always request a CTL file upon bootup, the phone proxy creates a database that marks the IP phones as secure. The entries in the secure phone database are removed after a specified configured timeout (via the <b>timeout secure-phones</b> command). Alternatively, you can use the <b>clear phone-proxy secure-phones</b> command to clear the phone proxy database without waiting for the configured timeout.</p> <p>This command is not supported in ASDM.</p>
H.239 Message Support in H.323 Application Inspection	<p>In this release, the ASA 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 ASA 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 preformed by ASN.1 coder.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard &gt; Rule Actions &gt; Protocol Inspection &gt; H.323 H.225. Click <b>Configure</b> and then choose the H.323 Inspect Map.</p>
Processing H.323 Endpoints When the Endpoints Do Not Send OLCAck	<p>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 ASA propagates OLC media proposal information into the media array and opens a pinhole for the media channel (extendedVideoCapability).</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard &gt; Rule Actions &gt; Protocol Inspection &gt; H.323 H.225.</p>
IPv6 in transparent firewall mode	<p>Transparent firewall mode now participates in IPv6 routing. Prior to this release, the ASA 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 ASA recognizes and passes IPv6 packets.</p> <p>All IPv6 functionality is supported unless specifically noted.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; Management IP Address.</p>

**Table 33**      **New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)**

Feature	Description
Botnet Traffic Filter	<p>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.”</p> <p><b>Note</b> This feature requires the Botnet Traffic Filter license. See the following licensing document for more information:</p> <p><a href="http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html">http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html</a></p> <p>The following commands were introduced: <b>dynamic-filter</b> commands (various), and the <b>inspect dns dynamic-filter-snoop</b> keyword.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Botnet Traffic Filter.</p>
AIP SSC card for the ASA 5505	<p>The AIP SSC offers IPS for the ASA 5505 ASA. Note that the AIP SSM does not support virtual sensors. The following commands were introduced: <b>allow-ssc-mgmt</b>, <b>hw-module module ip</b>, and <b>hw-module module allow-ip</b>.</p> <p>In ASDM, see Configuration &gt; Device Setup &gt; SSC Setup and Configuration &gt; IPS.</p>
IPv6 support for IPS	<p>You can now send IPv6 traffic to the AIP SSM or SSC when your traffic class uses the <b>match any</b> command, and the policy map specifies the <b>ips</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules.</p>
<b>Management Features</b>	
SNMP version 3 and encryption	<p>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).</p> <p>The following commands were introduced:</p> <ul style="list-style-type: none"> <li>• <b>show snmp engineid</b></li> <li>• <b>show snmp group</b></li> <li>• <b>show snmp-server group</b></li> <li>• <b>show snmp-server user</b></li> <li>• <b>snmp-server group</b></li> <li>• <b>snmp-server user</b></li> </ul> <p>The following command was modified:</p> <ul style="list-style-type: none"> <li>• <b>snmp-server host</b></li> </ul> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; SNMP.</p>
NetFlow	<p>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.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Logging &gt; Netflow.</p>
<b>Routing Features</b>	



**Table 33**      ***New Features for ASA Version 8.2(1)/ASDM Version 6.2(1) (continued)***

Feature	Description
Multicast NAT	The ASA now offers Multicast NAT support for group addresses.
<b>Troubleshooting Features</b>	
Coredump functionality	<p>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 ASA.</p> <p>To enable coredump, use the <b>coredump enable</b> command.</p>
<b>ASDM Features</b>	
ASDM Support for IPv6	All IPv6 functionality is supported unless specifically noted.
Support for Public Server configuration	<p>You can use ASDM to configure a public server. This allows to you define servers and services that you want to expose to an outside interface.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Public Servers.</p>

## New Features in Version 8.1

This section includes the following topics:

- [New Features in ASA 8.1\(2\)/ASDM 6.1\(5\), page 98](#)
- [New Features in ASA 8.1\(1\)/ASDM 6.1\(1\), page 101](#)

## New Features in ASA 8.1(2)/ASDM 6.1(5)

**Released: October 10, 2008**

[Table 34](#) lists the new features for ASA Version 8.1(2)/ASDM Version 6.1(5). This ASA software version is only supported on the ASA 5580.

**Table 34**      ***New Features for ASA Version 8.1(2)/ASDM Version 6.1(5)***

Feature	Description
<b>Remote Access Features</b>	
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 &gt; Firewall &gt; Advanced &gt; ACL Manager.</p>

**Table 34**      **New Features for ASA Version 8.1(2)/ASDM Version 6.1(5) (continued)**

Feature	Description
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 &gt; Remote Access VPN &gt; Certificate Management &gt; Identity Certificates &gt; 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 &gt; Device Management &gt; Certificate Management &gt; 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 <b>sysopt connection preserve-vpn-flows</b> command. This option is disabled by default.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; IPsec &gt; System Options. Check the <b>Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM)</b> checkbox to enable persistent IPsec tunneled flows.</p>
Show Active Directory Groups	<p>The CLI command <b>show ad-groups</b> 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 &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Dynamic Access Policies &gt; Add/Edit DAP &gt; Add/Edit AAA Attribute.</p>
Smart Tunnel over Mac OS	<p>Smart tunnels now support Mac OS.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Smart Tunnels.</p>
<b>Firewall Features</b>	
NetFlow Filtering	<p>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 <b>flow-export event-type</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Security Policy &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; NetFlow.</p>

**Table 34**      **New Features for ASA Version 8.1(2)/ASDM Version 6.1(5) (continued)**

Feature	Description
NetFlow Delay Flow Creation Event	<p>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 <b>flow-export delay flow-create</b> command.</p> <p><b>Note</b>    The teardown event includes all information regarding the flow; there is no loss of information.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Logging &gt; NetFlow.</p>
QoS Traffic Shaping	<p>If you have a device that transmits packets at a high speed, such as the ASA 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 <b>shape</b> command.</p> <p>See also the <b>crypto ipsec security-association replay</b> 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.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Security Policy &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.</p>
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"> <li>• TCP invalid ACK check (the <b>invalid-ack</b> command)</li> <li>• TCP packet sequence past window check (the <b>seq-past-window</b> command)</li> <li>• TCP SYN-ACK with data check (the <b>synack-data</b> command)</li> </ul> <p>You can also set the TCP out-of-order packet buffer timeout (the <b>queue</b> command <b>timeout</b> 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 <b>exceed-mss</b> 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"> <li>• Bad option length in TCP</li> <li>• TCP Window scale on non-SYN</li> <li>• Bad TCP window scale value</li> <li>• Bad TCP SACK ALLOW option</li> </ul> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; TCP Maps.</p>
TCP Intercept statistics	<p>You can enable collection for TCP Intercept statistics using the <b>threat-detection statistics tcp-intercept</b> command, and view them using the <b>show threat-detection statistics</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Threat Detection.</p>

**Table 34**      **New Features for ASA Version 8.1(2)/ASDM Version 6.1(5) (continued)**

Feature	Description
Threat detection shun timeout	You can now configure the shun timeout for threat detection using the <b>threat-detection scanning-threat shun duration</b> command.  In ASDM, see Configuration > Firewall > Threat Detection.
Threat detection host statistics fine tuning	You can now reduce the amount of host statistics collected, thus reducing the system impact of this feature, by using the <b>threat-detection statistics host number-of-rate</b> command.  In ASDM, see Configuration > Firewall > Threat Detection.
<b>Platform Features</b>	
Increased VLANs	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.
SNMP support for unnamed interfaces	Formerly, SNMP only provided information about interfaces that were configured using the <b>nameif</b> command. For example, SNMP only sent traps and performed walks on the IF MIB and IP MIB for interfaces that were named. SNMP was enhanced to show information about all physical interfaces and logical interfaces; a <b>nameif</b> command is no longer required to display the interfaces using SNMP.

## New Features in ASA 8.1(1)/ASDM 6.1(1)

**Released: March 1, 2008**

[Table 35](#) lists the new features for ASA Version 8.1(1)/ASDM Version 6.1(1). This ASA software version is only supported on the ASA 5580.

**Table 35**      **New Features for ASA Version 8.1(1)/ASDM Version 6.1(1)**

Feature	Description
Introduction of the Cisco ASA 5580	The Cisco ASA 5580 comes in two models: <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> In ASDM, see <b>Home &gt; System Resource Status</b> and <b>Home &gt; Device Information &gt; Environment Status</b> .
NetFlow	The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. For detailed information about this feature and the new CLI commands, see the <i>Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide</i> .  In ASDM, see <b>Configuration &gt; Device Management &gt; Logging &gt; Netflow</b> .

**Table 35**      **New Features for ASA Version 8.1(1)/ASDM Version 6.1(1) (continued)**

Feature	Description
Jumbo frame support	<p>The Cisco ASA 5580 supports jumbo frames when you enter the <b>jumbo-frame reservation</b> command. A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the the maximum use of other features, such as access lists.</p> <p>In ASDM, see <b>Configuration &gt; Device Setup &gt; Interfaces &gt; Add/Edit Interface &gt; Advanced</b>.</p>
Per-packet load balancing for multi-core ASAs	<p>For multi-core ASAs, the default behavior is to allow only one core to receive packets from an interface receive ring at a time. The <b>asp load-balance per-packet</b> command changes this behavior to allow multiple cores to receive packets from an interface receive ring and work on them independently. The default behavior is optimized for scenarios where packets are received uniformly on all interface rings.</p> <p>We introduced the following commands: <b>asp load-balance per-packet</b>, <b>show asp load-balance</b>.</p>
Timeout for SIP Provisional Media	<p>You can now configure the timeout for SIP provisional media using the <b>timeout sip-provisional-media</b> command.</p> <p>In ASDM, see <b>Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts</b>.</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 <b>show activation key detail</b> command.</p> <p>In ASDM in single context mode, see <b>Configuration &gt; Device Management &gt; System Image/Configuration &gt; Activation Key</b>. In ASDM in multiple context mode, see <b>System &gt; Configuration &gt; Device Management &gt; Activation Key</b>.</p>
New ASDM online help engine	<p>ASDM now supports a new look for the online help. The online help now maintains the topic-based selection of the user from the left bookmark pane while browsing through the right pane subject matter.</p>
ASDM CPU Core Usage Graph	<p>In single or multiple mode, the CPU core usage graph allows you to display the core CPU utilization status from the ASDM Home page.</p>
Intelligent platform management interface (IPMI) for ASDM	<p>Added support for intelligent platform management interface (IPMI), which provides the user with information on the status of the power supply, cooling fans, and temperature of the processors and chassis from the ASDM Home page.</p>
ASDM Assistant	<p>The ASDM Assistant is now available from <b>View</b> Menu, instead of the <b>Tools</b> Menu. The GUI has been changed to simplify the <b>Search</b> mechanism.</p>
ASDM Backup and Restore Enhancement	<p>The backup and restore enhancement allows you to back up configurations to the local machine and then restore them back on the server as necessary. Additionally, this feature backs up SSL VPN-related files. This feature is found in <b>Tools &gt; Backup Configuration</b>, and <b>Tools &gt; Restore Configuration</b>.</p> <p><i>Also supported for Version 8.0.</i></p>

**Table 35**      **New Features for ASA Version 8.1(1)/ASDM Version 6.1(1) (continued)**

Feature	Description
ASDM Log Viewer	The Log viewer enhancement displays the source and destination port information parsed from the syslog messages. This information is displayed on the <b>Monitoring &gt; Logging &gt; Real-Time Log Viewer</b> , and <b>Log Buffer</b> page. <i>Also supported for Version 8.0.</i>
Enhanced VPN Search in ASDM	Added a CLI command-based Search facility that offers intelligent hints while you are typing in keywords or a command. This search enhancement only exists on User Accounts, Connection Profiles, and Group Policies pages. <i>Also supported for Version 8.0.</i>

## New Features in Version 8.0

This section includes the following topics:

- [New Features in ASA 8.0\(5\)/ASDM 6.2\(3\), page 103](#)
- [New Features in ASA 8.0\(4\)/ASDM 6.1\(3\), page 105](#)
- [New Features in ASA 8.0\(3\)/ASDM 6.0\(3\), page 110](#)
- [New Features in ASA 8.0\(2\)/ASDM 6.0\(2\), page 115](#)


**Note**

There was no 8.0(1)/6.0(1) release.

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

**Released: November 3, 2009**

[Table 36](#) 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 36**      **New Features for ASA Version 8.0(5)/ASDM Version 6.2(3)**

Feature	Description
<b>Remote Access Features</b>	
Scalable Solutions for Waiting-to-Resume VPN Sessions	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: <b>Monitoring &gt; VPN &gt; VPN Statistics &gt; Sessions</b> . <i>Also available in Version 8.2(2).</i>
<b>Application Inspection Features</b>	

**Table 36**      **New Features for ASA Version 8.0(5)/ASDM Version 6.2(3) (continued)**

Feature	Description
Enabling Call Set up Between H.323 Endpoints	<p>You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The ASA includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages.</p> <p>Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the security appliance opens a pinhole through source IP address/port 0/0. By default, this option is disabled.</p> <p>The following command was introduced: <b>ras-rcf-pinholes enable</b>. Use this command during parameter configuration mode while creating an H.323 Inspection policy map.</p> <p>The following ASDM screen was modified: Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; H.323 &gt; Details &gt; State Checking.</p> <p><i>Also available in Version 8.2(2).</i></p>
<b>Interface Features</b>	
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	<p>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.</p> <p>The MAC addresses are also now persistent accross reloads.</p> <p>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.</p> <p>The following command was modified: <b>mac-address auto prefix</b> <i>prefix</i>.</p> <p>The following ASDM screen was modified: Configuration &gt; Context Management &gt; Security Contexts.</p> <p><i>Also available in Version 8.2(2).</i></p>
<b>High Availability Features</b>	
No notifications when interfaces are brought up or brought down during a switchover event	<p>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.</p> <p><i>Also available in Version 8.2(2).</i></p>
<b>Routing Features</b>	
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	<p>This enhancement introduces ASA 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 that is configured using the <b>dhcp-server</b> command, you can now configure the ASA to send the <b>subnet-selection</b> option, and the <b>link-selection</b> option or neither.</p> <p>The following ASDM screen was modified: Remote Access VPN &gt; Network Access &gt; IPsec connection profiles &gt; Add/Edit.</p> <p><i>Also available in Version 8.2(2).</i></p>
<b>SSM Features</b>	
CSC 6.3 Support in ASDM	<p>ASDM displays Web Reputation, User Group Policies, and User ID Settings in the Plus License listing on the main home page. CSC 6.3 security event enhancements are included, such as the new Web Reputation events and user and group identifications.</p>

## New Features in ASA 8.0(4)/ASDM 6.1(3)

Released: August 11, 2008

Table 37 lists the new features for ASA or PIX Version 8.0(4)/ASDM Version 6.1(3).

**Table 37** *New Features for ASA and PIX Version 8.0(4)/ASDM Version 6.1(3)*

Feature	Description
<b>Unified Communications Features<sup>1</sup></b>	
Phone Proxy	<p>Phone Proxy functionality is supported. ASA Phone Proxy provides similar features to those of the Metreos Cisco Unified Phone Proxy with additional support for SIP inspection and enhanced security. The ASA Phone Proxy has the following key features:</p> <ul style="list-style-type: none"> <li>• Secures remote IP phones by forcing the phones to encrypt signaling and media</li> <li>• Performs certificate-based authentication with remote IP phones</li> <li>• Terminates TLS signaling from IP phones and initiates TCP and TLS to Cisco Unified Mobility Advantage servers</li> <li>• Terminates SRTP and initiates RTP/SRTP to the called party</li> </ul> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; Phone Proxy.</p>
Mobility Proxy	<p>Secure connectivity (mobility proxy) between Cisco Unified Mobility Advantage clients and servers is supported.</p> <p>Cisco Unified Mobility Advantage solutions include the Cisco Unified Mobile Communicator, an easy-to-use software application for mobile handsets that extends enterprise communications applications and services to mobile phones and smart phones and the Cisco Unified Mobility Advantage server. The mobility solution streamlines the communication experience, enabling real-time collaboration across the enterprise.</p> <p>The ASA in this solution delivers inspection for the MMP (formerly called OLWP) protocol, the proprietary protocol between Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage. The ASA also acts as a TLS proxy, terminating and reoriginating the TLS signaling between the Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; TLS Proxy.</p>
Presence Federation Proxy	<p>Secure connectivity (presence federation proxy) between Cisco Unified Presence servers and Cisco/Microsoft Presence servers is supported. With the Presence solution, businesses can securely connect their Cisco Unified Presence clients back to their enterprise networks, or share Presence information between Presence servers in different enterprises.</p> <p>The ASA delivers functionality to enable Presence for Internet and intra-enterprise communications. An SSL-enabled Cisco Unified Presence client can establish an SSL connection to the Presence Server. The ASA enables SSL connectivity between server to server communication including third-party Presence servers communicating with Cisco Unified Presence servers. Enterprises share Presence information, and can use IM applications. The ASA inspects SIP messages between the servers.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; Protocol Inspection or Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; TLS Proxy &gt; Add &gt; Client Configuration.</p>
<b>Remote Access Features</b>	



**Table 37**      **New Features for ASA and PIX Version 8.0(4)/ASDM Version 6.1(3) (continued)**

Feature	Description
Auto Sign-On with Smart Tunnels for IE <sup>1</sup>	<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 Firewall &gt; Advanced &gt; ACL Manager.</p>
Entrust Certificate Provisioning <sup>1</sup>	<p>ASDM 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 &gt; Remote Access VPN &gt; Certificate Management &gt; Identity Certificates. Click <b>Enroll ASA SSL VPN head-end with Entrust</b>.</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 &gt; Device Management &gt; Certificate Management &gt; 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 <b>[no] sysopt connection preserve-vpn-flows</b> command. This option is disabled by default.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; IPsec &gt; System Options. Check the <b>Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM)</b> checkbox to enable persistent IPsec tunneled flows.</p>
Show Active Directory Groups	<p>The CLI command <b>show ad-groups</b> 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 &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Dynamic Access Policies &gt; Add/Edit DAP &gt; Add/Edit AAA Attribute.</p>

**Table 37**      **New Features for ASA and PIX Version 8.0(4)/ASDM Version 6.1(3) (continued)**

Feature	Description
Smart Tunnel over Mac OS <sup>1</sup>	Smart tunnels now support Mac OS.  In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels.
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in use is not being eliminated from the pool, the connection is not affected. However, if the address in use is being eliminated from the pool, the connection is brought down.  <i>Also available in Version 7.0(8) and 7.2(4).</i>
<b>Firewall Features</b>	
QoS Traffic Shaping	<p>If you have a device that transmits packets at a high speed, such as the ASA 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 <b>shape</b> command. See also the <b>crypto ipsec security-association replay</b> 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.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Security Policy &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.</p> <p><i>Also available in Version 7.2(4).</i></p>
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"> <li>• TCP invalid ACK check (the <b>invalid-ack</b> command)</li> <li>• TCP packet sequence past window check (the <b>seq-past-window</b> command)</li> <li>• TCP SYN-ACK with data check (the <b>synack-data</b> command)</li> </ul> <p>You can also set the TCP out-of-order packet buffer timeout (the <b>queue</b> command <b>timeout</b> 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 <b>exceed-mss</b> 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"> <li>• Bad option length in TCP</li> <li>• TCP Window scale on non-SYN</li> <li>• Bad TCP window scale value</li> <li>• Bad TCP SACK ALLOW option</li> </ul> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; TCP Maps.</p> <p><i>Also available in Version 7.2(4).</i></p>

**Table 37**      **New Features for ASA and PIX Version 8.0(4)/ASDM Version 6.1(3) (continued)**

Feature	Description
TCP Intercept statistics	You can enable collection for TCP Intercept statistics using the <b>threat-detection statistics tcp-intercept</b> command, and view them using the <b>show threat-detection statistics</b> command.  In ASDM 6.1(5) and later, see Configuration > Firewall > Threat Detection. This command was not supported in ASDM 6.1(3).
Threat detection shun timeout	You can now configure the shun timeout for threat detection using the <b>threat-detection scanning-threat shun duration</b> command.  In ASDM 6.1(5) and later, see Configuration > Firewall > Threat Detection. This command was not supported in ASDM 6.1(3).
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the <b>timeout sip-provisional-media</b> command.  In ASDM, see Configuration > Firewall > Advanced > Global Timeouts.  <i>Also available in Version 7.2(4).</i>
<b>clear conn</b> Command	The <b>clear conn</b> command was added to remove connections.  <i>Also available in Version 7.0(8) and 7.2(4).</i>
Fragment full reassembly	The <b>fragment</b> command was enhanced with the <b>reassemble full</b> keywords to enable full reassembly for fragments that are routed through the device. Fragments that terminate at the device are always fully reassembled.  <i>Also available in Version 7.0(8) and 7.2(4).</i>
Ethertype ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules are retained, but no new ones need to be added.  <i>Also available in Version 7.0(8) and 7.2(4).</i>
<b>Troubleshooting and Monitoring Features</b>	
<b>capture</b> command Enhancement	The <b>capture type asp-drop drop_code</b> command now accepts <b>all</b> as the <i>drop_code</i> , so you can now capture all packets that the ASA drops, including those dropped due to security checks.  <i>Also available in Version 7.0(8) and 7.2(4).</i>
<b>show asp drop</b> Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the <b>clear asp drop</b> command). It also displays the drop reason keywords next to the description, so you can easily use the <b>capture asp-drop</b> command using the keyword.  <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>clear asp table</b> Command	Added the <b>clear asp table</b> command to clear the hits output by the <b>show asp table</b> commands.  <i>Also available in Version 7.0(8) and 7.2(4).</i>
<b>show asp table classify hits</b> Command Enhancement	The <b>hits</b> option was added to the <b>show asp table classify</b> command, showing the timestamp indicating the last time the asp table counters were cleared. It also shows rules with hits values not equal to zero. This permits users to quickly see what rules are being hit, especially since a simple configuration may end up with hundreds of entries in the <b>show asp table classify</b> command.  <i>Also available in Version 7.0(8) and 8.0(4).</i>
MIB Enhancement	The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely.  <i>Also available in 8.0(4).</i>

**Table 37**      **New Features for ASA and PIX Version 8.0(4)/ASDM Version 6.1(3) (continued)**

Feature	Description
<b>show perfmon</b> Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Attempts, TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept.  <i>Also available in Version 7.0(8) and 7.2(4).</i>
<b>memory tracking</b> Commands	<p>The following new commands are introduced in this release:</p> <ul style="list-style-type: none"> <li>• <b>memory tracking enable</b>—This command enables the tracking of heap memory requests.</li> <li>• <b>no memory tracking enable</b>—This command disables tracking of heap memory requests, cleans up all currently gathered information, and returns all heap memory used by the tool itself to the system.</li> <li>• <b>clear memory tracking</b>—This command clears out all currently gathered information but continues to track further memory requests.</li> <li>• <b>show memory tracking</b>—This command shows currently allocated memory tracked by the tool, broken down by the topmost caller function address.</li> <li>• <b>show memory tracking address</b>—This command shows currently allocated memory broken down by each individual piece of memory. The output lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool.</li> <li>• <b>show memory tracking dump</b>—This command shows the size, location, partial callstack, and a memory dump of the given memory address.</li> <li>• <b>show memory tracking detail</b>—This command shows various internal details to be used in gaining insight into the internal behavior of the tool.</li> </ul> <p><i>Also available in Version 7.0(8) and 7.2(4).</i></p>
<b>Routing Features</b>	
IPv6 Multicast Listener Discovery Protocol v2 Support	<p>The ASA now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to discover the presence of multicast address listeners on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. The ASA becomes a multicast address listener, or a host, but not a a multicast router, and responds to Multicast Listener Queries and sends Multicast Listener Reports only.</p> <p>The following commands support this feature:</p> <ul style="list-style-type: none"> <li>• <b>clear ipv6 mld traffic</b> The <b>clear ipv6 mld traffic</b> command allows you to reset all the Multicast Listener Discovery traffic counters.</li> <li>• <b>show ipv6 mld traffic</b> The <b>show ipv6 mld</b> command allows you to display all the Multicast Listener Discovery traffic counters.</li> <li>• <b>debug ipv6 mld</b> The enhancement to the <b>debug ipv6</b> command allows the user to display the debug messages for MLD, to see whether the MLD protocol activities are working properly.</li> <li>• <b>show debug ipv6 mld</b> The enhancement to the <b>show debug ipv6</b> command allows the user to display whether <b>debug ipv6 mld</b> is enabled or disabled.</li> </ul> <p><i>Also available in Version 7.2(4).</i></p>

**Table 37**      **New Features for ASA and PIX Version 8.0(4)/ASDM Version 6.1(3) (continued)**

Feature	Description
<b>Platform Features</b>	
Native VLAN support for the ASA 5505	<p>You can now include the native VLAN in an ASA 5505 trunk port using the <b>switchport trunk native vlan</b> command.</p> <p>In ASDM, see Configuration &gt; Device Setup &gt; Interfaces &gt; Switch Ports &gt; Edit dialog.</p> <p><i>Also available in Version 7.2(4).</i></p>
SNMP support for unnamed interfaces	<p>Previously, SNMP only provided information about interfaces that were configured using the <b>nameif</b> command. For example, SNMP only sent traps and performed walks on the IF MIB and IP MIB for interfaces that were named. Because the ASA 5505 has both unnamed switch ports and named VLAN interfaces, SNMP was enhanced to show information about all physical interfaces and logical interfaces; a <b>nameif</b> command is no longer required to display the interfaces using SNMP. These changes affect all models, and not just the ASA 5505.</p>
<b>Failover Features</b>	
<b>failover timeout</b> Command	<p>The <b>failover timeout</b> command no longer requires a failover license for use with the static nailed feature.</p> <p><i>Also available in Version 7.0(8) and 7.2(4).</i></p>
<b>ASDM Features</b>	
Simplify DNS Panel	The DNS Panel on the ASDM GUI has been modified for ease of use. See <b>Configuration &gt; Device Management &gt; DNS</b> .
Redesign the File Transfer Dialog box	You can drag-and-drop files in the File Transfer dialog box. To access this dialog box, go to <b>Tools &gt; File Management</b> , and then click <b>File Transfer</b> .
Clear ACL Hit Counters	Added functionality enabling users to clear ACL hit counters. See the <b>Firewall &gt; Advanced &gt; ACL Manager</b> panel.
Renaming ACLs	<p>Added the ability to rename ACLs from ASDM.</p> <p>See the <b>Firewall &gt; Advanced &gt; ACL Manager</b> panel.</p>
Combine ASDM/HTTPS, SSH, Telnet into One Panel	ASDM has combined the ASDM, HTTPS, SSH, Telnet into one panel. See the <b>Monitoring &gt; Properties &gt; Device Access &gt; ASDM/HTTPS/Telnet/SSH Sessions</b> panel.
Display all standard ACLs in ACL Manager	<p>Added functionality enabling users to display all standard ACL in the ACL Manager.</p> <p>See the <b>Firewall &gt; Advanced &gt; ACL Manager</b> panel.</p>

1. This feature is not supported on the PIX security appliance.

## New Features in ASA 8.0(3)/ASDM 6.0(3)

Released: November 7, 2007

Table 38 lists the new features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3).

**Table 38**      **New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3)**

Feature	Description
<b>VPN Features</b>	
AnyConnect RSA SoftID API Integration	Provides support for AnyConnect VPN clients to communicate directly with RSA SoftID for obtaining user token codes. It also provides the ability to specify SoftID message support for a connection profile (tunnel group), and the ability to configure SDI messages on the security appliance that match SDI messages received through a RADIUS proxy. This feature ensures the prompts displayed to the remote client user are appropriate for the action required during authentication and the AnyConnect client responds successfully to authentication challenges.
IP Address Reuse Delay	<p>Delays the reuse of an IP address after it has been returned to the IP address pool. Increasing the delay prevents problems the security appliance may experience when an IP address is returned to the pool and reassigned quickly.</p> <p>In ASDM, see Configure &gt; Remote Access VPN &gt; Network (Client) Access &gt; Address Assignment &gt; Assignment Policy.</p>
Clientless SSL VPN Caching Static Content Enhancement	<p>There are two changes to the clientless SSL VPN caching commands:</p> <p>The <b>cache-compressed</b> command is deprecated.</p> <p>The new <b>cache-static-content</b> command configures the ASA to cache all static content, which means all cacheable Web objects that are not subject to SSL VPN rewriting. This includes content such as images and PDF files.</p> <p>The syntax of the command is <b>cache-static-content {enable   disable}</b>. By default, static content caching is disabled.</p> <p>Example:</p> <pre>hostname (config) # webvpn hostname (config-webvpn) # cache hostname (config-webvpn-cache) # cache-static-content enable hostname (config-webvpn-cache) #</pre> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Advanced &gt; Content Cache.</p> <p><i>Also available in Version 7.2(3).</i></p>
Smart Card Removal Disconnect	<p>This feature allows the central site administrator to configure remote client policy for deleting active tunnels when a Smart Card is removed. The Cisco VPN Remote Access Software clients (both IPsec and SSL) will, by default, tear down existing VPN tunnels when the user removes the Smart Card used for authentication. The following cli command disconnects existing VPN tunnels when a smart card is removed:</p> <p><b>smartcard-removal-disconnect {enable   disable}</b>. This option is enabled by default.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; Add/Edit Internal/External Group Policies &gt; More Options.</p> <p><i>Also available in Version 7.2(3).</i></p>

**Table 38**      **New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)**

Feature	Description
WebVPN load Balancing	<p>The adaptive security appliance now supports the use of FQDNs for load balancing. To perform WebVPN load balancing using FQDNs, you must enable the use of FQDNs for load balancing, enter the <b>redirect-fqdn enable</b> command. Then add an entry for each of your adaptive security appliance outside interfaces into your DNS server if not already present. Each adaptive security appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for reverse lookup. Enable DNS lookups on your adaptive security appliance with the <b>dns domain-lookup inside</b> command (or whichever interface has a route to your DNS server). Finally, you must define the ip address, of your DNS server on the adaptive security appliance. Following is the new CLI associated with this enhancement: <b>redirect-fqdn {enable   disable}</b>.</p> <p>In ASDM, see Configuration &gt; VPN &gt; Load Balancing.</p> <p><i>Also available in Version 7.2(3).</i></p>
<b>Application Inspection Features</b>	
WAAS and ASA Interoperability	<p>The <b>inspect waas</b> command is added to enable WAAS inspection in the policy-map class configuration mode. This CLI is integrated into Modular Policy Framework for maximum flexibility in configuring the feature. The <b>[no] inspect waas</b> command can be configured under a default inspection class and under a custom class-map. This inspection service is not enabled by default.</p> <p>The keyword option waas is added to the <b>show service-policy inspect</b> command to display WAAS statistics.</p> <pre>show service-policy inspect waas</pre> <p>A new system log message is generated when WAAS optimization is detected on a connection. All L7 inspection services including IPS are bypassed on WAAS optimized connections.</p> <p>System Log Number and Format:</p> <pre>%ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection.</pre> <p>A new connection flag "W" is added in the WAAS connection. The <b>show conn detail</b> command is updated to reflect the new flag.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; Protocol Inspection.</p> <p><i>Also available in Version 7.2(3).</i></p>
DNS Guard Enhancement	<p>Added an option to enable or disable DNS guard. When enabled, this feature allows only one DNS response back from a DNS request.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; Inspect maps &gt; DNS.</p> <p><i>Also available in Version 7.2(3).</i></p>

**Table 38**      **New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)**

Feature	Description
Support for ESMTP over TLS	<p>This enhancement adds the configuration parameter <b>allow-tls [action log]</b> in the esmtp policy map. By default, this parameter is not enabled. When it is enabled, ESMTP inspection would not mask the 250-STARTTLS echo reply from the server nor the <b>STARTTLS</b> command from the client. After the server replies with the 220 reply code, the ESMTP inspection turns off by itself; the ESMTP traffic on that session is no longer inspected. If the <b>allow-tls action log</b> parameter is configured, the syslog message ASA-6-108007 is generated when TLS is started on an ESMTP session.</p> <pre>policy-map type inspect esmtp esmtp_map parameters allow-tls [action log]</pre> <p>A new line for displaying counters associated with the <b>allow-tls</b> parameter is added to the <b>show service-policy inspect esmtp</b> command. It is only present if <b>allow-tls</b> is configured in the policy map. By default, this parameter is not enabled.</p> <pre>show service-policy inspect esmtp allow-tls, count 0, log 0</pre> <p>This enhancement adds a new system log message for the <b>allow-tls</b> parameter. It indicates on an esmtp session the server has responded with a 220 reply code to the client <b>STARTTLS</b> command. The ESMTP inspection engine will no longer inspect the traffic on this connection.</p> <p>System log Number and Format:</p> <pre>%ASA-6-108007: TLS started on ESMTP session between client &lt;client-side interface-name&gt;:&lt;client IP address&gt;/&lt;client port&gt; and server &lt;server-side interface-name&gt;:&lt;server IP address&gt;/&lt;server port&gt;</pre> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; Inspect Map &gt; ESMTP.</p> <p><i>Also available in Version 7.2(3).</i></p>
<b>High Availability Features</b>	
Added Dataplane Keepalive Mechanism	<p>You can now configure the ASA so that a failover will not occur if the AIP SSM is upgraded. In previous releases when two ASAs with AIP SSMs are configured in failover and the AIP SSM software is updated, the ASA triggers a failover, because the AIP SSM needs to reboot or restart for the software update to take effect.</p> <p><i>Also available in Version 7.0(7) and 7.2(3)</i></p>
Fully Qualified Domain Name Support Enhancement	<p>Added option in the <b>redirect-fqdn</b> command to send either the fully qualified domain name (FQDN) or the IP address to the client in a VPN load balancing cluster.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; High Availability &gt; VPN Load Balancing or Configuration &gt; Remote Access VPN &gt; Load Balancing.</p>
<b>DHCP Features</b>	



**Table 38**      **New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)**

Feature	Description
DHCP client ID enhancement	<p>If you enable the DHCP client for an interface using the <b>ip address dhcp</b> command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use this new command to include the interface MAC address for option 61. If you do not configure this command, the client ID is as follows:  cisco-&lt;MAC&gt;-&lt;interface&gt;-&lt;hostname&gt;.</p> <p>We introduced the following command: <b>dhcp-client client-id interface interface_name</b></p> <p>We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Server; then click <b>Advanced</b>.</p> <p><i>Also available in Version 7.2(3).</i></p>
DHCP client broadcast flag	<p>If you enable the DHCP client for an interface using the <b>ip address dhcp</b> command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.</p> <p>If you enter the <b>no dhcp-client broadcast-flag</b> command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address.</p> <p>The DHCP client can receive both broadcast and unicast offers from the DHCP server.</p> <p>We introduced the following command: <b>dhcp-client broadcast-flag</b></p> <p>We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Server; then click <b>Advanced</b>.</p>
<b>Platform Features</b>	
ASA 5510 Security Plus License Allows Gigabit Ethernet for Port 0 and 1	<p>The ASA 5510 ASA now has the security plus license to enable GE (Gigabit Ethernet) for port 0 and 1. If you upgrade the license from base to security plus, the capacity of the external port Ethernet0/0 and Ethernet0/1 increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the <b>speed</b> command to change the speed on the interface and use the <b>show interface</b> command to see what speed is currently configured for each interface.</p> <p><i>Also available in Version 7.2(3).</i></p>
ASA 5505 Increased VLAN range	<p>The ASA 5505 ASA now supports VLAN IDs between 1 and 4090. Originally, only VLAN IDs between 1 and 1001 were supported.</p> <p><i>Also available in Version 7.2(3).</i></p>
<b>Troubleshooting Features</b>	
<b>capture</b> Command Enhancement	<p>The enhancement to the <b>capture</b> command allows the user to capture traffic and display it in real time. It also allows the user to specify command line options to filter traffic without having to configure a separate access list. This enhancement adds the <b>real-time</b> and five-tuple <b>match</b> options.</p> <p><b>capture cap_name [real-time] [dump] [detail [trace] [match prot {host ip   ip mask   any} [{eq   lt   gt} port] {host ip   ip mask   any} [{eq   lt   gt} port]]</b></p> <p><i>Also available in Version 7.2(3).</i></p>
<b>ASDM Features</b>	

**Table 38**      **New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)**

Feature	Description
ASDM banner enhancement	<p>The adaptive security appliance software supports an ASDM banner. If configured, when you start ASDM, this banner text will appear in a dialog box with the option to continue or disconnect. The Continue option dismisses the banner and completes login as usual whereas, the Disconnect option dismisses the banner and terminates the connection. This enhancement requires the customer to accept the terms of a written policy before connecting.</p> <p>Following is the new CLI associated with this enhancement:</p> <pre><b>banner {exec   login   motd   asdm} text</b> <b>show banner [exec   login   motd   asdm]</b> <b>clear banner</b></pre> <p>In ASDM, see Configuration &gt; Properties &gt; Device Administration &gt; Banner.</p> <p><i>Also available in Version 7.2(3).</i></p>
Localization Enhancement in ASDM	<p>ASDM is now enhanced to supports AnyConnect Localization. See <b>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Customization</b>, or on the <b>Configuration &gt; RemoteAccess &gt; Network Access &gt; AnyConnect Customization and Configuration &gt; RemoteAccess &gt; Language Localization &gt; MST Translation panel</b>.</p>
Time-based License Enhancement	<p>On the Home page, the License tab of the Device Dashboard tab now includes the number of days until a time-based license expires (if applicable).</p>
Network Objects	<p>You can now add true network objects that you can use in firewall rules. Objects can be named, and when you edit an object, the change is inherited wherever the object is used. Also, when you create a rule, the networks that you specify in the rule are automatically added to the network object list so you can reuse them elsewhere. You can name and edit these automatic entries as well. See <b>Configuration &gt; Firewall &gt; Objects &gt; Network Objects/Groups</b>.</p>
Client Software Location Enhancement	<p>Added support in Client Software Location list to allow client updates from Linux or Mac systems. See <b>Configure &gt; Remote Access VPN &gt; Language Localization</b>.</p> <p><i>Also available in Version 7.2(3).</i></p>
CSC Event and Statistic Reporting Enhancement	<p>With the Cisco Content Security and Control (CSC) 6.2 software, ASDM provides events and statistics for the new Damage Cleanup Services (DCS) feature. DCS removes malware from clients and servers and repairs system registries and memory.</p>

## New Features in ASA 8.0(2)/ASDM 6.0(2)

**Released: June 18, 2007**

[Table 39](#) lists the new features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2).



### Note

There was no 8.0(1)/6.0(1) release.

**Table 39**      ***New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2)***

<b>Feature</b>	<b>Description</b>
<b>Routing Features</b>	
EIGRP routing	The ASA supports EIGRP or EIGRP stub routing.
<b>High Availability Features</b>	
Remote command execution in Failover pairs	You can execute commands on the peer unit in a failover pair without having to connect directly to the peer. This works for both Active/Standby and Active/Active failover.
CSM configuration rollback support	Adds support for the Cisco Security Manager configuration rollback feature in failover configurations.
Failover pair Auto Update support	You can use an Auto Update server to update the platform image and configuration in failover pairs.
Stateful Failover for SIP signaling	SIP media and signaling connections are replicated to the standby unit.
Redundant interfaces	A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the ASA reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to eight redundant interface pairs.
<b>Module Features</b>	
Virtual IPS sensors with the AIP SSM	The AIP SSM running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode adaptive security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.
Password reset	You can reset the password on the SSM hardware module.
<b>VPN Authentication Features<sup>1</sup></b>	
Combined certificate and username/password login	An administrator requires a username and password in addition to a certificate for login to SSL VPN connections.
Internal domain username/password	Provides a password for access to internal resources for users who log in with credentials other than a domain username and password, for example, with a one-time password. This is a password in addition to the one a user enters when logging in.
Generic LDAP support	This includes OpenLDAP and Novell LDAP. Expands LDAP support available for authentication and authorization.
Onscreen keyboard	The ASA includes an onscreen keyboard option for the login page and subsequent authentication requests for internal resources. This provides additional protection against software-based keystroke loggers by requiring a user to use a mouse to click characters in an onscreen keyboard for authentication, rather than entering the characters on a physical keyboard.
SAML SSO verified with RSA Access Manager	The ASA supports Security Assertion Markup Language (SAML) protocol for Single Sign On (SSO) with RSA Access Manager (Cleartrust and Federated Identity Manager).
NTLMv2	Version 8.0(2) adds support for NTLMv2 authentication for Windows-based clients.

**Table 39**      ***New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)***

<b>Feature</b>	<b>Description</b>
<b>Certificate Features</b>	
Local certificate authority	Provides a certificate authority on the ASA for use with SSL VPN connections, both browser- and client-based.
OCSP CRL	Provides OCSP revocation checking for SSL VPN.
<b>Cisco Secure Desktop Features</b>	
Host Scan	<p>As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection, the remote computer scans for a greatly expanded collection of antivirus and antispyware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the ASA. The ASA uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP).</p> <p>With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements.</p> <p>Cisco can provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop.</p>
Simplified prelogin assessment and periodic checks	Cisco Secure Desktop now simplifies the configuration of prelogin and periodic checks to perform on remote Microsoft Windows computers. Cisco Secure Desktop lets you add, modify, remove, and place conditions on endpoint checking criteria using a simplified, graphical view of the checks. As you use this graphical view to configure sequences of checks, link them to branches, deny logins, and assign endpoint profiles, Cisco Secure Desktop Manager records the changes to an XML file. You can configure the ASA to use returned results in combination with many other types of data, such as the connection type and multiple group settings, to generate and apply a DAP to the session.
<b>VPN Access Policy Features</b>	
Dynamic access policies (DAP)	<p>VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.</p> <p>Dynamic Access Policies (DAP) on the ASA let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the ASA grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.</p>

**Table 39**      ***New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)***

<b>Feature</b>	<b>Description</b>
Administrator differentiation	Lets you differentiate regular remote access users and administrative users under the same database, either RADIUS or LDAP. You can create and restrict access to the console via various methods (TELNET and SSH, for example) to administrators only. It is based on the IETF RADIUS service-type attribute.
<b>Platform Enhancements</b>	
VLAN support for remote access VPN connections	Provides support for mapping (tagging) of client traffic at the group or user level. This feature is compatible with clientless as well as IPsec and SSL tunnel-based connections.
VPN load balancing for the ASA 5510	Extends load balancing support to ASA 5510 adaptive security appliances that have a Security Plus license.
Crypto conditional debug	Lets users debug an IPsec tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPsec operations and reducing the amount of debug output, you can better troubleshoot the ASA with a large number of tunnels.
<b>Browser-based SSL VPN Features</b>	
Enhanced portal design	Version 8.0(2) includes an enhanced end user interface that is more cleanly organized and visually appealing.
Customization	Supports administrator-defined customization of all user-visible content.
Support for FTP	You can provide file access via FTP in addition to CIFS (Windows-based).
Plugin applets	Version 8.0(2) adds a framework for supporting TCP-based applications without requiring a pre-installed client application. Java applets let users access these applications from the browser-enabled SSL VPN portal. Initial support is for TELNET, SSH, RDP, and VNC.
Smart tunnels	<p>A smart tunnel is a connection between an application and a remote site, using a browser-based SSL VPN session with the ASA as the pathway. Version 8.0(2) lets you identify the applications to which you want to grant smart tunnel access, and lets you specify the path to the application and the SHA-1 hash of its checksum to check before granting it access. Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access.</p> <p>The remote host originating the smart tunnel connection must be running Microsoft Windows Vista, Windows XP, or Windows 2000, and the browser must be enabled with Java, Microsoft ActiveX, or both.</p>
RSS newsfeed	Administrators can populate the clientless portal with RSS newsfeed information, which lets company news or other information display on a user screen.
Personal bookmark support	Users can define their own bookmarks. These bookmarks are stored on a file server.
Transformation enhancements	Adds support for several complex forms of web content over clientless connections, including Adobe flash and Java WebStart.
IPv6	Allows access to IPv6 resources over a public IPv4 connection.

**Table 39**      ***New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)***

<b>Feature</b>	<b>Description</b>
Web folders	Lets browser-based SSL VPN users connecting from Windows operating systems browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.
Microsoft Sharepoint enhancement	Extends Web Access support for Microsoft Sharepoint, integrating Microsoft Office applications available on the machine with the browser to view, change, and save documents shared on a server. Version 8.0(2) supports Windows Sharepoint Services 2.0 in Windows Server 2003.
<b>HTTP/HTTPS Proxy Features</b>	
PAC support	Lets you specify the URL of a proxy autoconfiguration file (PAC) to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL.
Proxy exclusion list	Lets you configure a list of URLs to exclude from the HTTP requests the ASA can send to an external proxy server.
<b>VPN Network Access Control Features</b>	
SSL VPN tunnel support	The ASA provides NAC posture validation of endpoints that establish AnyConnect VPN client sessions.
Support for audit services	You can configure the ASA to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server uses the host IP address to challenge the host directly to assess its health. For example, it might challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host. If the token indicates the remote host is healthy, the posture validation server sends a network access policy to the ASA for application to the traffic on the tunnel.
<b>Application Inspection Features</b>	
Modular policy framework inspect class map	Traffic can match one of multiple match commands in an inspect class map; formerly, traffic had to match all match commands in a class map to match the class map.
AIC for encrypted streams and AIC Arch changes	Provides HTTP inspection into TLS, which allows AIC/MPF inspection in WebVPN HTTP and HTTPS streams.
TLS Proxy for SCCP and SIP <sup>2</sup>	Enables inspection of encrypted traffic. Implementations include SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with the Cisco CallManager.
SIP enhancements for CCM	Improves interoperability with CCM 5.0 and 6.x with respect to signaling pinholes.
IPv6 support for SIP	The SIP inspection engine supports IPv6 addresses. IPv6 addresses can be used in URLs, in the Via header field, and SDP fields.
Full RTSP PAT support	Provides TCP fragment reassembly support, a scalable parsing routine on RTSP, and security enhancements that protect RTSP traffic.
<b>Access List Features</b>	

**Table 39**      ***New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)***

<b>Feature</b>	<b>Description</b>
Enhanced service object group	Lets you configure a service object group that contains a mix of TCP services, UDP services, ICMP-type services, and any protocol. It removes the need for a specific ICMP-type object group and protocol object group. The enhanced service object group also specifies both source and destination services. The access list CLI now supports this behavior.
Ability to rename access list	Lets you rename an access list.
Live access list hit counts	Includes the hit count for ACEs from multiple access lists. The hit count value represents how many times traffic hits a particular access rule.
<b>Attack Prevention Features</b>	
Set connection limits for management traffic to the adaptive security appliance	For a Layer 3/4 management class map, you can specify the <b>set connection</b> command.
Threat detection	You can enable basic threat detection and scanning threat detection to monitor attacks such as DoS attacks and scanning attacks. For scanning attacks, you can automatically shun attacking hosts. You can also enable scan threat statistics to monitor both valid and invalid traffic for hosts, ports, protocols, and access lists.
<b>NAT Features</b>	
Transparent firewall NAT support	You can configure NAT for a transparent firewall.
<b>Monitoring Features</b>	
Secure logging	You can enable secure connections to the syslog server using SSL or TLS with TCP, and encrypted system log message content. Not supported on the PIX series adaptive security appliance.
<b>ASDM Features</b>	
Redesigned Interface	Reorganizes information to provide greater logical consistency and ease of navigation.
Expanded onscreen help	ASDM describes features and configuration options on screen, which reduces the need to consult other information sources.
Visual policy editor	The visual policy editor lets an administrator configure access control policies and posture checking.
Firewall Dashboard	From the home page, you can now track threats to your network by monitoring traffic that exceeds rate limits, as well as allowed and dropped traffic by host, access list, port, or protocol.
Accessibility Features	Features such as keyboard navigation, alternate text for graphics, and improved screen reader support have been added.
Complex Configuration Support	You can move between panes without applying changes, allowing you to enter multi-pane configurations before applying that configuration to the device.
Device List	ASDM maintains a list of recently accessed devices, allowing you to switch between devices and contexts.
SSL VPN configuration wizard	The new SSL VPN configuration wizard provides step-by-step guidance in configuring basic SSL VPN connections.
Startup Wizard Enhancement	The Startup Wizard now allows you to configure the adaptive ASA to pass traffic to an installed CSC SSM.
ASDM Assistant Enhancements <sup>4</sup>	An assistant for configuring Secure Voice was added.

**Table 39**      ***New Features for ASA and PIX Version 8.0(2)/ASDM Version 6.0(2) (continued)***

Feature	Description
Packet Capture Wizard	The Packet Capture Wizard assists you in obtaining and downloading sniffer trace in PCAP format.
Service Policy Rule Wizard	Updated to support IPS Virtualization.
Certificate Management Enhancements	The certificate management GUI is reorganized and simplified.

1. Clientless SSL VPN features are not supported on the PIX security appliance.
2. TLS proxy is not supported on the PIX security appliance.

## New Features in Version 7.2

This section includes the following topics:

- [New Features in ASA 7.2\(5\)/ASDM 5.2\(5\), page 121](#)
- [New Features in ASA 7.2\(4\)/ASDM 5.2\(4\), page 121](#)
- [New Features in ASA 7.2\(3\)/ASDM 5.2\(3\), page 125](#)
- [New Features in ASA 7.2\(2\)/ASDM 5.2\(2\), page 129](#)
- [New Features in ASA 7.2\(1\)/ASDM 5.2\(1\), page 131](#)

### New Features in ASA 7.2(5)/ASDM 5.2(5)

**Released: May 11, 2010**

There were no new features in ASA 7.2(5)/ASDM 5.2(5)

### New Features in ASA 7.2(4)/ASDM 5.2(4)

**Released: April 7, 2008**

[Table 21](#) lists the new features for ASA and PIX Version 7.2(4)/ASDM Version 5.2(4).

**Table 40**      ***New Features for ASA and PIX Version 7.2(4)/ASDM Version 5.2(4)***

Feature	Description
<b>Remote Access Features</b>	
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in use is not being eliminated from the pool, the connection is not affected. However, if the address in use is being eliminated from the pool, the connection is brought down. <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>Routing Features</b>	



**Table 40**      **New Features for ASA and PIX Version 7.2(4)/ASDM Version 5.2(4) (continued)**

Feature	Description
IPv6 Multicast Listener Discovery Protocol v2 Support	<p>The ASA now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to discover the presence of multicast address listeners on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. The ASA becomes a multicast address listener, or a host, but not a multicast router, and responds to Multicast Listener Queries and sends Multicast Listener Reports only.</p> <p>The following commands support this feature:</p> <ul style="list-style-type: none"> <li>• <b>clear ipv6 mld traffic</b> The <b>clear ipv6 mld traffic</b> command allows you to reset all the Multicast Listener Discovery traffic counters.</li> <li>• <b>show ipv6 mld traffic</b> The <b>show ipv6 mld</b> command allows you to display all the Multicast Listener Discovery traffic counters.</li> <li>• <b>debug ipv6 mld</b> The enhancement to the <b>debug ipv6</b> command allows the user to display the debug messages for MLD, to see whether the MLD protocol activities are working properly.</li> <li>• <b>show debug ipv6 mld</b> The enhancement to the <b>show debug ipv6</b> command allows the user to display whether <b>debug ipv6 mld</b> is enabled or disabled.</li> </ul> <p><i>Also available in Version 8.0(4).</i></p>
<b>Platform Features</b>	
Native VLAN Support on ASA 5505 Trunk Ports	<p>You can now allow native VLANs on a trunk port (see the <b>switchport trunk native vlan</b> command).</p> <p>In ASDM, see Configuration &gt; Device Setup &gt; Interfaces &gt; Switch Ports &gt; Edit dialog.</p> <p><i>Also available in Version 8.0(4).</i></p>
<b>Connection Features</b>	
<b>clear conn</b> Command	<p>The <b>clear conn</b> command was added to remove connections.</p> <p><i>Also available in Version 7.0(8) and 8.0(4).</i></p>
Fragment full reassembly	<p>The <b>fragment</b> command was enhanced with the <b>reassemble full</b> keywords to enable full reassembly for fragments that are routed through the device. Fragments that terminate at the device are always fully reassembled.</p> <p><i>Also available in Version 7.0(8) and 8.0(4).</i></p>

**Table 40**      **New Features for ASA and PIX Version 7.2(4)/ASDM Version 5.2(4) (continued)**

Feature	Description
QoS Traffic Shaping	<p>If you have a device that transmits packets at a high speed, such as the ASA 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 <b>shape</b> command. See also the <b>crypto ipsec security-association replay</b> command, which lets you configure the IPSec anti-replay window size.</p> <p>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 feature avoids possible false alarms.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Security Policy &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.</p> <p><i>Also available in Version 8.0(4).</i></p>
<b>Firewall Features</b>	
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"> <li>• TCP invalid ACK check (the <b>invalid-ack</b> command)</li> <li>• TCP packet sequence past window check (the <b>seq-past-window</b> command)</li> <li>• TCP SYN-ACK with data check (the <b>synack-data</b> command)</li> </ul> <p>You can also set the TCP out-of-order packet buffer timeout (the <b>queue</b> command <b>timeout</b> 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 <b>exceed-mss</b> 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"> <li>• Bad option length in TCP</li> <li>• TCP Window scale on non-SYN</li> <li>• Bad TCP window scale value</li> <li>• Bad TCP SACK ALLOW option</li> </ul> <p>In ASDM, see the Configuration &gt; Global Objects &gt; TCP Maps pane.</p> <p><i>Also available in Version 8.0(4).</i></p>
Timeout for SIP Provisional Media	<p>You can now configure the timeout for SIP provisional media using the <b>timeout sip-provisional-media</b> command.</p> <p>In ASDM, see the Configuration &gt; Properties &gt; Timeouts pane.</p> <p><i>Also available in Version 8.0(4).</i></p>
Ethertype ACL MAC Enhancement	<p>EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules are retained, but no new ones need to be added.</p> <p><i>Also available in Version 7.0(8) and 8.0(4).</i></p>
<b>Troubleshooting and Monitoring Features</b>	

**Table 40**      **New Features for ASA and PIX Version 7.2(4)/ASDM Version 5.2(4) (continued)**

Feature	Description
<b>capture</b> command Enhancement	The <b>capture type asp-drop</b> <i>drop_code</i> command now accepts <b>all</b> as the <i>drop_code</i> , so you can now capture all packets that the ASA drops, including those dropped due to security checks. <i>Also available in Version 7.0(8) and 8.0(4).</i>
MIB Enhancement	The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely. <i>Also available in 8.0(4).</i>
<b>show asp drop</b> Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the <b>clear asp drop</b> command). It also displays the drop reason keywords next to the description, so you can easily use the <b>capture asp-drop</b> command using the keyword. <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>clear asp table</b> Command	Added the <b>clear asp table</b> command to clear the hits output by the <b>show asp table</b> commands. <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>show asp table classify hits</b> Command Enhancement	The <b>hits</b> option was added to the <b>show asp table classify</b> command, showing the timestamp indicating the last time the asp table counters were cleared. It also shows rules with hits values not equal to zero. This permits users to quickly see what rules are being hit, especially since a simple configuration may end up with hundreds of entries in the <b>show asp table classify</b> command. <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>show perfmon</b> Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Attempts, TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept. <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>memory tracking</b> Commands	The following new commands are introduced in this release: <ul style="list-style-type: none"> <li>• <b>memory tracking enable</b>—This command enables the tracking of heap memory requests.</li> <li>• <b>no memory tracking enable</b>—This command disables tracking of heap memory requests, cleans up all currently gathered information, and returns all heap memory used by the tool itself to the system.</li> <li>• <b>clear memory tracking</b>—This command clears out all currently gathered information but continues to track further memory requests.</li> <li>• <b>show memory tracking</b>—This command shows currently allocated memory tracked by the tool, broken down by the topmost caller function address.</li> <li>• <b>show memory tracking address</b>—This command shows currently allocated memory broken down by each individual piece of memory. The output lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool.</li> <li>• <b>show memory tracking dump</b>—This command shows the size, location, partial callstack, and a memory dump of the given memory address.</li> <li>• <b>show memory tracking detail</b>—This command shows various internal details to be used in gaining insight into the internal behavior of the tool.</li> </ul> <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>Failover Features</b>	

**Table 40**      **New Features for ASA and PIX Version 7.2(4)/ASDM Version 5.2(4) (continued)**

Feature	Description
<b>failover timeout</b> Command	The <b>failover timeout</b> command no longer requires a failover license for use with the static nailed feature.  <i>Also available in Version 7.0(8) and 8.0(4).</i>
<b>ASDM Features</b>	
Network Objects	You can now add true network objects that you can use in firewall rules. Objects can be named, and when you edit an object, the change is inherited wherever the object is used. Also, when you create a rule, the networks that you specify in the rule are automatically added to the network object list so you can reuse them elsewhere. You can name and edit these automatic entries as well. See Configuration > Objects > Network Objects/Groups.
Enhanced ASDM Rule Table	The ASDM rule tables have been redesigned to streamline policy creation.

## New Features in ASA 7.2(3)/ASDM 5.2(3)

**Released: August 15, 2007**

[Table 21](#) lists the new features for ASA and PIX Version 7.2(3)/ASDM Version 5.2(3).

**Table 41**      **New Features for ASA and PIX Version 7.2(3)/ASDM Version 5.2(3)**

Feature	Description
<b>Remote Access Features</b>	
WebVPN load Balancing	The adaptive security appliance now supports the use of FQDNs for load balancing. To perform WebVPN load balancing using FQDNs, you must enable the use of FQDNs for load balancing, enter the <b>redirect-fqdn enable</b> command. Then add an entry for each of your adaptive security appliance outside interfaces into your DNS server if not already present. Each adaptive security appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for reverse lookup. Enable DNS lookups on your adaptive security appliance with the <b>dns domain-lookup inside</b> command (or whichever interface has a route to your DNS server). Finally, you must define the ip address, of your DNS server on the adaptive security appliance. Following is the new CLI associated with this enhancement: <b>redirect-fqdn {enable   disable}.</b>  In ASDM, see Configuration > VPN > Load Balancing.  <i>Also available in Version 8.0(3).</i>

**Table 41**      **New Features for ASA and PIX Version 7.2(3)/ASDM Version 5.2(3) (continued)**

Feature	Description
Clientless SSL VPN Caching Static Content Enhancement	<p>There are two changes to the clientless SSL VPN caching commands:</p> <p>The <b>cache-compressed</b> command is deprecated.</p> <p>The new <b>cache-static-content</b> command configures the ASA to cache all static content, which means all cacheable Web objects that are not subject to SSL VPN rewriting. This includes content such as images and PDF files.</p> <p>The syntax of the command is <b>cache-static-content {enable   disable}</b>. By default, static content caching is disabled.</p> <p>Example:</p> <pre>hostname (config) # webvpn hostname (config-webvpn) # cache hostname (config-webvpn-cache) # cache-static-content enable hostname (config-webvpn-cache) #</pre> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Advanced &gt; Content Cache.</p> <p><i>Also available in Version 8.0(3).</i></p>
Smart Card Removal Disconnect	<p>This feature allows the central site administrator to configure remote client policy for deleting active tunnels when a Smart Card is removed. The Cisco VPN Remote Access Software clients (both IPSec and SSL) will, by default, tear down existing VPN tunnels when the user removes the Smart Card used for authentication. The following cli command disconnects existing VPN tunnels when a smart card is removed: <b>smartcard-removal-disconnect {enable   disable}</b>. This option is enabled by default.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; Add/Edit Internal/External Group Policies &gt; More Options.</p> <p><i>Also available in Version 8.0(3).</i></p>
<b>Platform Features</b>	
ASA 5510 Security Plus License Allows Gigabit Ethernet for Port 0 and 1	<p>The ASA 5510 ASA now has the security plus license to enable GE (Gigabit Ethernet) for port 0 and 1. If you upgrade the license from base to security plus, the capacity of the external port Ethernet0/0 and Ethernet0/1 increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the <b>speed</b> command to change the speed on the interface and use the <b>show interface</b> command to see what speed is currently configured for each interface.</p> <p><i>Also available in Version 8.0(3).</i></p>
ASA 5505 Increased VLAN range	<p>The ASA 5505 ASA now supports VLAN IDs between 1 and 4090. Originally, only VLAN IDs between 1 and 1001 were supported.</p> <p><i>Also available in Version 8.0(3).</i></p>
<b>Troubleshooting Features</b>	
<b>capture</b> Command Enhancement	<p>The enhancement to the <b>capture</b> command allows the user to capture traffic and display it in real time. It also allows the user to specify command line options to filter traffic without having to configure a separate access list. This enhancement adds the <b>real-time</b> and five-tuple <b>match</b> options.</p> <pre><b>capture</b> cap_name [<b>real-time</b>] [<b>dump</b>] [<b>detail</b> [<b>trace</b>] [<b>match</b> prot {<b>host ip</b>   <b>ip mask</b>   <b>any</b>} [{<b>eq</b>   <b>lt</b>   <b>gt</b>} port] {<b>host ip</b>   <b>ip mask</b>   <b>any</b>} [{<b>eq</b>   <b>lt</b>   <b>gt</b>} port]]</pre> <p><i>Also available in Version 8.0(3).</i></p>

**Table 41**      **New Features for ASA and PIX Version 7.2(3)/ASDM Version 5.2(3) (continued)**

Feature	Description
<b>Application Inspection Features</b>	
Support for ESMTP over TLS	<p>This enhancement adds the configuration parameter <b>allow-tls [action log]</b> in the esmtp policy map. By default, this parameter is not enabled. When it is enabled, ESMTP inspection would not mask the 250-STARTTLS echo reply from the server nor the <b>STARTTLS</b> command from the client. After the server replies with the 220 reply code, the ESMTP inspection turns off by itself; the ESMTP traffic on that session is no longer inspected. If the <b>allow-tls action log</b> parameter is configured, the syslog message ASA-6-108007 is generated when TLS is started on an ESMTP session.</p> <pre>policy-map type inspect esmtp esmtp_map parameters allow-tls [action log]</pre> <p>A new line for displaying counters associated with the <b>allow-tls</b> parameter is added to the <b>show service-policy inspect esmtp</b> command. It is only present if <b>allow-tls</b> is configured in the policy map. By default, this parameter is not enabled.</p> <pre>show service-policy inspect esmtp allow-tls, count 0, log 0</pre> <p>This enhancement adds a new system log message for the <b>allow-tls</b> parameter. It indicates on an esmtp session the server has responded with a 220 reply code to the client <b>STARTTLS</b> command. The ESMTP inspection engine will no longer inspect the traffic on this connection.</p> <p>System log Number and Format:</p> <pre>%ASA-6-108007: TLS started on ESMTP session between client &lt;client-side interface-name&gt;:&lt;client IP address&gt;/&lt;client port&gt; and server &lt;server-side interface-name&gt;:&lt;server IP address&gt;/&lt;server port&gt;</pre> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; Inspect Map &gt; ESMTP.</p> <p><i>Also available in Version 8.0(3).</i></p>
DNS Guard Enhancement	<p>Added an option to enable or disable DNS guard. When enabled, this feature allows only one DNS response back from a DNS request.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; Inspect maps &gt; DNS.</p> <p><i>Also available in Version 8.0(3).</i></p>

**Table 41**      **New Features for ASA and PIX Version 7.2(3)/ASDM Version 5.2(3) (continued)**

Feature	Description
WAAS and ASA Interoperability	<p>The <b>inspect waas</b> command is added to enable WAAS inspection in the policy-map class configuration mode. This CLI is integrated into Modular Policy Framework for maximum flexibility in configuring the feature. The <b>[no] inspect waas</b> command can be configured under a default inspection class and under a custom class-map. This inspection service is not enabled by default.</p> <p>The keyword option <b>waas</b> is added to the <b>show service-policy inspect</b> command to display WAAS statistics.</p> <pre>show service-policy inspect waas</pre> <p>A new system log message is generated when WAAS optimization is detected on a connection. All L7 inspection services including IPS are bypassed on WAAS optimized connections.</p> <p>System Log Number and Format:</p> <pre>%ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection.</pre> <p>A new connection flag "W" is added in the WAAS connection. The <b>show conn detail</b> command is updated to reflect the new flag.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; Protocol Inspection.</p> <p><i>Also available in Version 8.0(3).</i></p>
<b>DHCP Features</b>	
DHCP client ID enhancement	<p>If you enable the DHCP client for an interface using the <b>ip address dhcp</b> command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use this new command to include the interface MAC address for option 61. If you do not configure this command, the client ID is as follows: <code>cisco-&lt;MAC&gt;-&lt;interface&gt;-&lt;hostname&gt;</code>.</p> <p>We introduced the following command: <b>dhcp-client client-id interface interface_name</b></p> <p>We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Server; then click <b>Advanced</b>.</p> <p><i>Also available in Version 8.0(3).</i></p>
<b>Module Features</b>	
Added Dataplane Keepalive Mechanism	<p>You can now configure the ASA so that a failover will not occur if the AIP SSM is upgraded. In previous releases when two ASAs with AIP SSMs are configured in failover and the AIP SSM software is updated, the ASA triggers a failover, because the AIP SSM needs to reboot or restart for the software update to take effect.</p> <p><i>Also available in Version 7.0(7) and 8.0(3)</i></p>
<b>ASDM Features</b>	

**Table 41**      ***New Features for ASA and PIX Version 7.2(3)/ASDM Version 5.2(3) (continued)***

Feature	Description
ASDM banner enhancement	<p>The adaptive security appliance software supports an ASDM banner. If configured, when you start ASDM, this banner text will appear in a dialog box with the option to continue or disconnect. The Continue option dismisses the banner and completes login as usual whereas, the Disconnect option dismisses the banner and terminates the connection. This enhancement requires the customer to accept the terms of a written policy before connecting.</p> <p>Following is the new CLI associated with this enhancement:</p> <pre><b>banner {exec   login   motd   asdm} text</b></pre> <pre><b>show banner [exec   login   motd   asdm]</b></pre> <pre><b>clear banner</b></pre> <p>In ASDM, see Configuration &gt; Properties &gt; Device Administration &gt; Banner.</p> <p><i>Also available in Version 8.0(3).</i></p>
Cisco Content Security and Control (CSC) Damage Cleanup Services (DCS) feature events and statistics	<p>With the Cisco Content Security and Control (CSC) 6.2 software, ASDM provides events and statistics for the new Damage Cleanup Services (DCS) feature. DCS removes malware from clients and servers and repairs system registries and memory.</p>
Client Software Location	<p>Added support in Client Software Location list to allow client updates from Linux or Mac systems. In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; IPsec &gt; Upload Software &gt; Client Software.</p> <p><i>Also available in Version 8.0(3).</i></p>

## New Features in ASA 7.2(2)/ASDM 5.2(2)

**Released: November 22, 2006**

[Table 21](#) lists the new features for ASA and PIX Version 7.2(2)/ASDM Version 5.2(2).

**Table 42**      ***New Features for ASA and PIX Version 7.2(2)/ASDM Version 5.2(2)***

Feature	Description
<b>Module Features</b>	
Password reset on SSMs	<p>You can reset the password on the AIP-SSM and CSC-SSM of user 'cisco' back to the default value 'cisco'.</p> <p>We added the following command: <b>hw-module module password-reset.</b></p>
<b>AAA Features</b>	



**Table 42**      **New Features for ASA and PIX Version 7.2(2)/ASDM Version 5.2(2) (continued)**

Feature	Description
HTTP(S) authentication challenge flexible configuration	<p>The new <b>aaa authentication listener</b> command enables the ASA to authenticate web pages and select the form-based redirection approach that is currently used in Version 7.2(1).</p> <p>7.2(2) reintroduces the choice to use basic HTTP authentication that was available before 7.2(1). Basic HTTP and HTTPS authentication generates custom login windows. You can use basic HTTP authentication if:</p> <ul style="list-style-type: none"> <li>You do not want the adaptive security appliance to open listening ports</li> <li>You use NAT on a router and you do not want to create a translation rule for the web page served by the adaptive security appliance</li> <li>Basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.</li> </ul> <p><b>Note</b> By default the <b>aaa authentication listener</b> command is not present in the configuration, making Version 7.1 <b>aaa</b> behavior the default for 7.2(2). However, when a Version 7.2(1) configuration is upgraded to Version 7.2(2), the appropriate <b>aaa authentication listener</b> commands are added to the configuration so that the <b>aaa</b> behavior will not be changed by the upgrade.</p> <p>To support basic HTTP, the <b>virtual http</b> command was restored. This is needed with basic authentication when you have cascading authentication requests.</p> <p>In Version 7.2(1), basic authentication was replaced by a form based authentication approach where HTTP and HTTPS connections are redirected to authentication pages that are served from the ASA. After successful authentication, the browser is again redirected to the originally-intended URL. This was done to provide:</p> <ul style="list-style-type: none"> <li>More graceful support authentication challenge processing</li> <li>An identical authentication experience for http and https users</li> </ul> <p>A persistent logon/logoff URL for network users This approach does require listening ports to be opened on the ASA on each interface on which <b>aaa authentication</b> was enabled.</p>
<b>Interface Features</b>	
Maximum number of VLANs increased	<p>The maximum number of VLANs for the Security Plus license on the ASA 5505 adaptive security appliance was increased from 5 (3 fully functional; 1 failover; one restricted to a backup interface) to 20 fully functional interfaces. In addition, the number of trunk ports was increased from 1 to 8. Now there are 20 fully functional interfaces, you do not need to use the backup interface command to cripple a backup ISP interface; you can use a fully-functional interface for it. The <b>backup interface</b> command is still useful for an Easy VPN configuration.</p> <p>VLAN limits were also increased for the ASA 5510 adaptive security appliance (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 adaptive security appliance (from 100 to 150), the ASA 5550 adaptive security appliance (from 200 to 250).</p>
Increased physical interfaces on the ASA 5510 base license	On the ASA Model 5510, the maximum number of physical interfaces available has been changed from 3+1 to unlimited (5).
<b>Certification Features</b>	
FIPS 140-2	7.2(2) has been submitted for FIPS 140 Level 2 validation.

**Table 42** *New Features for ASA and PIX Version 7.2(2)/ASDM Version 5.2(2) (continued)*

Feature	Description
<b>ASDM Features</b>	
Multicast support	Support for the following multicast commands has been added: <ul style="list-style-type: none"> <li>• <b>mfib forwarding</b></li> <li>• <b>multicast boundary</b></li> <li>• <b>pim bidir-neighbor-filter</b></li> <li>• <b>pim neighbor-filter</b></li> <li>• <b>pim old-register-checksum</b></li> </ul>
Local demo mode	ASDM works when it is connected to a device in a local demo mode.

## New Features in ASA 7.2(1)/ASDM 5.2(1)

**Released: May 31, 2006**

[Table 21](#) lists the new features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1).

**Table 43** *New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1)*

Feature	Description
<b>Platform Features</b>	
ASA 5505 support	<p>The ASA 5505 was introduced in this release. The ASA 5505 is a new model for small office/home office, enterprise teleworker environments, includes a built-in 8-port Fast Ethernet switch, and supports Easy VPN, Dual ISP, and has many more features</p> <p>The ASA 5505 has Power over Ethernet (PoE) switch ports that can be used for PoE devices, such as IP phones. However, these ports are not restricted to that use. They can also be used as Ethernet switch ports. If a PoE device is not attached, power is not supplied to the port.</p>
ASA 5550 support	The ASA 5550 delivers gigabit-class security services and enables Active/Active high availability for large enterprise and service-provider networks in a reliable, 1RU form-factor. Providing gigabit connectivity in the form of both Ethernet- and Fiber-based interfaces with high-density VLAN integration, the ASA 5550 enables businesses to segment their networks into numerous high-performance zones for improved security.
<b>Easy VPN Features (ASA 5505 Only)</b>	
Client Mode (also called Port Address Translation) and Network Extension Mode	<ul style="list-style-type: none"> <li>• <b>Client Mode</b>—Hides the IP addresses of devices on the ASA 5505 private network, so that all traffic from the ASA 5505 private network arrives on the private network of the central-site ASA with a single-source, assigned IP address. You cannot ping or access a device on the ASA 5505 private network from the central site, but you can access the assigned IP address.</li> <li>• <b>Network Extension Mode</b>—Permits devices behind the ASA to have direct access to devices on the ASA 5505 private network only through the tunnel. You can ping or access a device on the ASA 5505 network from the central site.</li> </ul> <p>The ASA 5505 does not have a default mode; you must specify the one that you want to use.</p>
Automatic Tunnel Initiation	Supports NEM, but not Client Mode. It uses a group name, username, and password stored in the configuration to initiate the tunnel.

**Table 43**      ***New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
IKE and IPsec Support	The ASA 5505 supports preshared keys and certificates (RSA-SIG). The ASA uses IKE Aggressive Mode for preshared keys and IKE Main Mode for RSA-SIG based key exchange. Cisco ASA 5505 can initiate IPsec, IPsec over NAT-T, and IPsec over cTCP sessions.
Secure Unit Authentication (SUA)	Supports the ASA 5505 authentication with dynamically generated authentication credentials or with static credentials to be entered at tunnel initiation. With SUA enabled, the user must manually trigger the IKE tunnel using a browser or an interactive CLI.
Individual User Authentication (IUA)	Enables static and one-time password authentication of individual clients on the inside network. IUA and SUA are independent of each other; they work in combination or isolation from each other.
Token-Based Authentication	Supports Security Dynamics (SDI) SecurID one-time passwords.
Authentication by HTTP Redirection	Redirects unauthenticated HTTP traffic to a login page if SUA or a username and password are not configured or if IUA is disabled.
Load Balancing	<p>An ASA 5505 configured with dual ISP backup supports cluster-based VPN load balancing over the two Ethernet ports available in the Internet zone. The load-balancing scheme involves a “virtual director” IP address that is the destination of incoming client connections. The server that share a virtual director IP address form a cluster, where one cluster member acts as the cluster master. The master receives a request sent to the virtual director and redirects the client, using a proprietary IKE notify message, to the optimal server in the cluster. The current ISAKMP session terminates, and a new session is attempted to the optimal server.</p> <p>If the connection to the optimal server fails, the client reconnects to the primary server (at the virtual director IP address of the cluster) and repeats the load-balancing procedure. If the connection to the primary server fails, the client rolls over to the next configured backup server, which may be the master of another cluster.</p>
Failover (using Backup Server List)	You can configure a list of 10 backup servers in addition to the primary server. The ASA 5505 attempts to establish a tunnel with the primary server. If that attempt fails, the ASA 5505 attempts to establish a tunnel with other specified servers in the backup server list in sequence.
Device Pass-Through	<p>Encompasses both IP Phone Pass Through and LEAP Pass Through features.</p> <p>Certain devices, such as printers and Cisco IP phones, are incapable of performing authentication, so they cannot participate in IUA. With device pass-through enabled, the ASA 5505 exempts these devices from authentication if IAU is enabled.</p> <p>The Easy VPN Remote feature identifies the devices to exempt, based on a configured list of MAC addresses. A related issue exists with wireless devices such as wireless access points and wireless nodes. These devices require LEAP/PEAP authentication to let wireless nodes participate in the network. It is only after the LEAP/PEAP authentication stage that the wireless nodes can perform IUA. The ASA 5505 also bypasses LEAP/PEAP packets when you enable Device Pass Through, so that the wireless nodes can participate in IUA.</p>
IKE Mode Configuration	You can set the attribute values that the ASA 5505 requests after IKE Phase I and XAUTH. The device at the central site downloads the VPN policy and the ASA 5505 dynamically configures the features based on the security values. Except for SUA, the Clear Save password, and the backup concentrator list, the dynamic feature configuration lasts only while the tunnel is up.
Remote Management	Supports management of the ASA 5505 over the tunnel to the outside interface with NEM configured, and in the clear to the outside interface.
DNS Resolution of Easy VPN Peer Names	The ASA 5505 resolves the Easy VPN peer names with the DNS server. You can specify the DNS name of the server/client in the CLI.

**Table 43**      ***New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
Split tunneling	Allows the client decide which traffic to send over the tunnel, based on a configured list of networks accessible by tunneling to the central site. Traffic destined to a network other than those listed in the split tunnel network list is sent out in the clear. A zero-length list indicates no split tunneling, and all traffic travels over the tunnel.
Push Banner	Allows you to configure a 491-byte banner message to display in HTTP form to individual users who try to authenticate using IUA.
<b>Application Inspection Features</b>	
Enhanced ESMTP Inspection	This feature allows you to detect attacks, including spam, phishing, malformed message attacks, and buffer overflow and underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detects several attacks, blocks senders and receivers, and blocks mail relay.
DCERPC Inspection	<p>This feature allows you to change the default configuration values used for DCERPC application inspection using a DCERPC inspect map.</p> <p>DCERPC is a protocol used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.</p> <p>Typically, a client queries a server called the Endpoint Mapper (EPM) that listens on a well-known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance that provides the service. The security appliance allows the appropriate port number and network address and also applies NAT or PAT, if needed, for the secondary connection.</p>
Enhanced NetBIOS Inspection	<p>This feature allows you to change the default configuration values used for NetBIOS application inspection.</p> <p>NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service packets and NetBIOS datagram services packets. It also enforces protocol conformance by checking the various count and length fields for consistency.</p>
Enhanced H.323 Inspection	<p>This feature allows you to change the default configuration values used for H.323 application inspection.</p> <p>H.323 inspection supports RAS, H.225, and H.245, and its functionality translates all embedded IP addresses and ports. It performs state tracking and filtering and can do a cascade of inspect function activation. H.323 inspection supports phone number filtering, dynamic T.120 control, H.245 tunneling control, protocol state tracking, H.323 call duration enforcement, and audio and video control.</p>
Enhanced DNS Inspection	This feature allows you to specify actions when a message violates a parameter that uses a DNS inspection policy map. DNS application inspection supports DNS message controls that provide protection against DNS spoofing and cache poisoning. User configurable rules allow filtering based on the DNS header, domain name, and resource record TYPE and CLASS.

**Table 43**      ***New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
Enhanced FTP Inspection	<p>This feature allows you to change the default configuration values used for FTP application inspection.</p> <p>FTP command filtering and security checks are provided using strict FTP inspection for improved security and control. Protocol conformance includes packet length checks, delimiters and packet format checks, command terminator checks, and command validation.</p> <p>Blocking FTP based on user values is also supported so that it is possible for FTP sites to post files for download but restrict access to certain users. You can block FTP connections based on file type, server name, and other attributes. System message logs are generated if an FTP connection is denied after inspection.</p>
Enhanced HTTP Inspection	<p>This feature allows you to change the default configuration values used for HTTP application inspection.</p> <p>HTTP application inspection scans HTTP headers and body and performs various checks on the data. These checks prevent various HTTP constructs, content types, and tunneling and messaging protocols from traversing the security appliance.</p> <p>HTTP application inspection can block tunneled applications and non-ASCII characters in HTTP requests and responses, preventing malicious content from reaching the web server. Size limiting of various elements in HTTP request and response headers, URL blocking, and HTTP server header type spoofing are also supported.</p>
Enhanced Skinny (SCCP) Inspection	<p>This feature allows you to change the default configuration values used for SCCP (Skinny) application inspection.</p> <p>Skinny application inspection performs translation of embedded IP address and port numbers within the packet data and dynamic opening of pinholes. It also performs additional protocol conformance checks and basic state tracking.</p>
Enhanced SIP Inspection	<p>This feature allows you to change the default configuration values used for SIP application inspection.</p> <p>SIP is a widely used protocol for Internet conferencing, telephony, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats.</p> <p>SIP application inspection provides address translation in the message header and body, dynamic opening of ports, and basic sanity checks. It also supports application security and protocol conformance, which enforces the sanity of the SIP messages, as well as detects SIP-based attacks.</p>
Instant Messaging (IM) Inspection	<p>This feature allows you to change the default configuration values used for Instant Messaging (IM) application inspection.</p> <p>Instant Messaging (IM) application inspection provides detailed access control to control network usage. It also helps stop leakage of confidential data and propagations of network threats. A regular expression database search that represents various patterns for Instant Messaging (IM) protocols to be filtered is applied. A syslog is generated if the flow is not recognized.</p> <p>The scope can be limited by using an access list to specify any traffic streams to be inspected. For UDP messages, a corresponding UDP port number is also configurable. Inspection of Yahoo! Messenger and MSN Messenger instant messages are supported.</p>

**Table 43**      ***New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
MPF-Based Regular Expression Classification Map	This feature allows you to define regular expressions in Modular Policy Framework class maps and match a group of regular expressions that has the <b>match-any</b> attribute. You can use a regular expression class map to match the content of certain traffic; for example, you can match URL strings inside HTTP packets.
Radius Accounting Inspection	This feature allows you to protect against an over-billing attack in the Mobile Billing Infrastructure. The <b>policy-map type inspect radius-accounting</b> command was introduced in this version.
GKRCS Support for H.323	Two control signaling methods are described in the ITU-T H.323 recommendation: Gatekeeper Routed Control Signaling (GKRCS) and Direct Call Signalling (DCS). DCS is supported by the Cisco IOS gatekeeper. This feature adds Gatekeeper Routed Control Signaling (GKRCS) control signaling method support.
Skinny Video Support	This feature adds SCCP version 4.1.2 message support to print the message name processed by the inspect feature when <b>debug skinny</b> is enabled. CCM 4.0.1 messages are supported.
SIP IP Address Privacy	<p>This feature allows you to retain the outside IP addresses embedded in inbound SIP packets for all transactions, except REGISTER (because it is exchanged between the proxy and the phone), to hide the real IP address of the phone. The REGISTER message and the response to REGISTER message will be exempt from this operation because this message is exchanged between the phone and the proxy.</p> <p>When this feature is enabled, the outside IP addresses in the SIP header and SDP data of inbound SIP packets will be retained. Use the <b>ip-address-privacy</b> command to turn on this feature.</p>
RTP/RTCP Inspection	<p>This feature NATs embedded IP addresses and opens pinholes for RTP and RTCP traffic. This feature ensures that only RTP packets flow on the pinholes opened by Inspects SIP, Skinny, and H.323.</p> <p>To prevent a malicious application from sending UDP traffic to make use of the pinholes created on the ASA, this feature allows you to monitor RTP and RTCP traffic and to enforce the validity of RTP and RTCP packets.</p>

**Remote Access and Site-to-Site VPN Features**

**Table 43**      ***New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)***

Feature	Description
Network Admission Control	<p>Network Admission Control (NAC) allows you to validate a peer based on its state. This method is referred to as posture validation (PV). PV can include verifying that the peer is running applications with the latest patches, and ensuring that the antivirus files, personal firewall rules, or intrusion protection software that runs on the remote host are up to date.</p> <p>An Access Control Server (ACS) must be configured for Network Admission Control before you configure NAC on the ASA.</p> <p>As a NAC authenticator, the ASA does the following:</p> <ul style="list-style-type: none"> <li>• Initiates the initial exchange of credentials based on IPsec session establishment and periodic exchanges thereafter.</li> <li>• Relays credential requests and responses between the peer and the ACS.</li> <li>• Enforces the network access policy for an IPsec session based on results from the ACS server.</li> <li>• Supports a local exception list based on the peer operating system, and optionally, an ACL.</li> <li>• (Optional) Requests access policies from the ACS server for a clientless host.</li> </ul> <p>As an ACS client, the ASA supports the following:</p> <ul style="list-style-type: none"> <li>• EAP/RADIUS</li> <li>• RADIUS attributes required for NAC</li> </ul> <p>NAC on the ASA differs from NAC on Cisco IOS Layer 3 devices (such as routers) where routers trigger PV based on routed traffic. The ASA enabled with NAC uses an IPsec VPN session as the trigger for PV. Cisco IOS routers configured with NAC use an Intercept ACL to trigger PV based on traffic destined for certain networks. Because external devices cannot access the network behind the ASA without starting a VPN session, the ASA does not need an intercept ACL as a PV trigger. During PV, all IPsec traffic from the peer is subject to the default ACL configured for the peer's group.</p> <p>Unlike the Cisco VPN 3000 Concentrator Series, NAC on the ASA supports stateless failover, initialization of all NAC sessions in a tunnel group, revalidation of all NAC sessions in a tunnel group, and posture validation exemption lists configured for each tunnel group. NAC on the ASA does not support non-VPN traffic, IPv6, security contexts, and WebVPN.</p> <p>By default, NAC is disabled. You can enable it on a group policy basis.</p>

**Table 43**      ***New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
L2TP Over IPsec	<p>Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clients to use the public IP network to communicate securely with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data. L2TP is based on the client/server model. The function is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator (LAC). The LNS typically runs on a network gateway such as a router, while the LAC can be a dial-up Network Access Server (NAS), or a PC with a bundled L2TP client such as Microsoft Windows 2000.</p> <p>L2TP/IPsec provides the capability to deploy and administer an L2TP VPN solution alongside the IPsec VPN and firewall services in a single platform.</p> <p>The primary benefit of configuring L2TP with IPsec in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, enabling remote access from virtually anyplace with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN). No additional client software, such as Cisco VPN client software, is required.</p>
OCSP Support	The Online Certificate Status Protocol (OCSP) provides an alternative to CRL for obtaining the revocation status of X.509 digital certificates. Rather than requiring a client to download a complete and often large certificate revocation list, OCSP localizes the certificate status on a Validation Authority, which it queries for the status of a specific certificate.
Multiple L2TP Over IPsec Clients Behind NAT	The security appliance can successfully establish remote-access L2TP-over-IPsec connections to more than one client behind one or more NAT devices. This enhances the reliability of L2TP over IPsec connections in typical SOHO/branch office environment environments, where multiple L2TP over IPsec clients must communicate securely with a central office.
Nokia Mobile Authentication Support	You can establish a VPN using a handheld Nokia 92xx Communicator series cellular device for remote access. The authentication protocol that these devices use is the IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) protocol.
Zonelabs Integrity Server	You can configure the ASA in a network that deploys the Zone Labs Integrity System to enforce security policies on remote VPN clients. In this case, the ASA is an edge gateway between the Zone Labs Integrity server and the remote clients. The Zone Labs Integrity server and the Zone Labs Personal Firewall on the remote client ensure that a remote client complies with a centrally managed security policy before the client can access private network resources. You configure the ASA to pass security policy information between the server and clients to maintain or close client connections to prevent a server connection failure, and to optionally, require SSL certificate authentication of both the Integrity server and the ASA.
Hybrid XAUTH	You can configure hybrid authentication to enhance the IKE security between the ASA and remote users. With this feature, IKE Phase I requires two steps. The ASA first authenticates to the remote VPN user with standard public key techniques and establishes an IKE security association that is unidirectionally authenticated. An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use any one of the supported authentication methods. Hybrid XAUTH allows you to use digital certificates for ASA authentication and a different method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID.
IPsec Fragmentation and Reassembly Statistics	You can monitor additional IPsec fragmentation and reassembly statistics that help to debug IPsec-related fragmentation and reassembly issues. The new statistics provide information about fragmentation and reassembly both before and after IPsec processing.



**Table 43**      **New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)**

Feature	Description
Inspection IPS, CSC and URL Filtering for WebVPN	<p>This feature adds support for inspection, IPS, and Trend Micro for WebVPN traffic in clientless mode and port forwarding mode. Support for SVC mode is preexisting. In all of the modes, the Trend Micro and the IPS engines will be triggered (if configured).</p> <p>URL/FTP/HTTPS/Java/Activex filtering using WebSense and N2H2 support has also been added. DNS inspect will be triggered for the DNS requests.</p> <p>In port forwarding mode, HTTP, SMTP, FTP, and DNS inspections with the filtering mechanisms using WebSense and N2H2 support has been added.</p>
<b>Routing Features</b>	
Active RIP Support	<p>The ASA supports RIP Version 1 and RIP Version 2. You can only enable one RIP routing process on the ASA. When you enable the RIP routing process, RIP is enabled on all interfaces. By default, the security appliance sends RIP Version 1 updates and accepts RIP Version 1 and Version 2 updates.</p> <p>To specify the version of RIP accepted on an interface, use the <b>rip receive version</b> command in interface configuration mode.</p>
Standby ISP Support	This feature allows you to configure a link standby ISP if the link to your primary ISP fails. It uses static routing and object tracking to determine the availability of the primary route and to activate the secondary route when the primary route fails.
PPPoE Client	Point-to-Point Protocol over Ethernet (PPPoE) combines two widely accepted standards, Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. PPPoE clients are typically personal computers connected to an ISP over a remote broadband connection, such as DSL or cable service. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use.
Dynamic DNS Support	<p>You can create dynamic DNS (DDNS) update methods and configure them to update the Resource Records (RRs) on the DNS server at whatever frequency you need.</p> <p>DDNS complements DHCP, which enables users to dynamically and transparently assign reusable IP addresses to clients. DDNS then provides dynamic updating and synchronizing of the name to the address and the address to the name mappings on the DNS server. With this version, the ASA supports the IETF standard for DNS record updates.</p>
Multicast Routing Enhancements	Multicast routing enhancements allows you to define multicast boundaries so that domains with RPs that have the same IP address do not leak into each other, to filter PIM neighbors to better control the PIM process, and to filter PIM bidir neighbors to support mixed bidirectional and sparse-mode networks.
Expanded DNS Domain Name Usage	You can use DNS domain names, such as www.example.com, when configuring AAA servers and also with the <b>ping</b> , <b>traceroute</b> , and <b>copy</b> commands.
Intra-Interface Communication for Clear Traffic	You can now allow any traffic to enter and exit the same interface, and not just VPN traffic.
IPv6 Security Enforcement of IPv6 Addresses	This feature allows you to configure the security appliance to require that IPv6 addresses for directly connected hosts use the Modified EUI-64 format for the interface identifier portion of the address.
<b>Multiple Context Mode Features</b>	

**Table 43**      ***New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)***

<b>Feature</b>	<b>Description</b>
Private and Automatic MAC Address Assignments and Generation for Multiple Context Mode	<p>You can assign a private MAC address (both active and standby for failover) for each interface. For multiple context mode, you can automatically generate unique MAC addresses for shared context interfaces, which makes classifying packets into contexts more reliable.</p> <p>The new <b>mac-address auto</b> command allows you to automatically assign private MAC addresses to each shared context interface.</p>
Resource Management for Security Contexts	If you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.
Save All Context Configurations from the System	You can now save all context configurations at once from the system execution space using the <b>write memory all</b> command.
<b>High Availability Features</b>	
Sub-second Failover	This feature allows you to configure failover to detect and respond to failures in under a second.
Configurable Prompt	With this feature, the user can see the failover status of the security appliance without having to enter the <b>show failover</b> command and parse the output. This feature allows users to see the chassis slot number of the failover unit. Previously, the prompt reflected just the hostname, security context, and configuration mode. The <b>prompt</b> command provides support for this feature.
<b>Firewall Features</b>	
Generic Input Rate Limiting	<p>This feature prevents denial of service (DoS) attacks on a ASA or on certain inspection engines on a firewall. The 7.0 release supports egress rate-limiting (police) functionality and in this release, input rate-limiting functionality extends the current egress policing functionality.</p> <p>The <b>police</b> command is extended for this functionality.</p>
Authentication for Through Traffic and Management Access Supports All Servers Previously Supported for VPN Clients	All server types can be used for firewall authentication with the following exceptions: HTTP Form protocol supports single sign-on authentication for WebVPN users only and SDI is not supported for HTTP administrative access.
Dead Connection Detection (DCD)	This feature allows the adaptive security appliance to automatically detect and expire dead connections. In previous versions, dead connections never timed out; they were given an infinite timeout. Manual intervention was required to ensure that the number of dead connections did not overwhelm the security appliance. With this feature, dead connections are detected and expired automatically, without interfering with connections that can still handle traffic. The set connection timeout and show service-policy commands provide DCD support.
WCCP	The Web Cache Communication Protocol (WCCP) feature allows you to specify WCCP service groups and redirect web cache traffic. The feature transparently redirects selected types of traffic to a group of web cache engines to optimize resource usage and lower response times.
<b>Filtering Features</b>	
URL Filtering Enhancements for Secure Computing (N2H2)	This feature allows you to enable long URL, HTTPS, and FTP filtering by using both Websense (the current vendor) and N2H2 (a vendor that has been purchased by Secure Computing). Previously, the code only enabled the vendor Websense to provide this type of filtering. The url-block, url-server, and filter commands provide support for this feature.
<b>Management and Troubleshooting Features</b>	

**Table 43**      **New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)**

Feature	Description
Auto Update	The security appliance can now be configured as an Auto Update server in addition to being configured as an Auto Update client. The existing <b>client-update</b> command (which is also used to update VPN clients) is enhanced to support the new Auto Update server functionality, and includes new keywords and arguments that the security appliance needs to update security appliances configured as clients. For the security appliance configured as an Auto Update client, the auto-update command continues to be the command used to configure the parameters that the security appliance needs to communicate with the Auto Update server.
Modular Policy Framework Support for Management Traffic	You can now define a Layer 3/4 class map for to-the-security-appliance traffic, so you can perform special actions on management traffic. For this version, you can inspect RADIUS accounting traffic.
Traceroute	The <b>traceroute</b> command allows you to trace the route of a packet to its destination.
Packet Tracer	<p>The packet tracer tool allows you to trace the life span of a packet through the ASA to see if it is behaving as expected.</p> <p>The <b>packet-tracer</b> command provides detailed information about the packets and how they are processed by the security appliance. If a command from the configuration did not cause the packet to drop, the <b>packet-tracer</b> command will provide information about the cause.</p> <p>The new patent-pending Packet Tracer tool in ASDM lets you easily trace the life span of a packet through the ASA in an animated packet flow model to see if it is behaving as expected and simplify troubleshooting no matter how complex the network design. The tool provides the attributes of a packet such as source and destination IP addresses with a visual representation of the different phases of the packet and the relevant configuration, which is accessible with a single click. For each phase, it displays whether the packet is dropped or allowed.</p>
<b>ASDM Features</b>	
Enhanced ASDM rules table	<p>The ASDM rule tables have been redesigned to streamline policy creation. In addition to simplified rule creation that maps more closely with CLI, the rule tables support most configuration scenarios including super-netting and using an object group that is associated to more than interface. The use of ASDM location and ASDM group was removed to simplify the creation of rules. You now have the ability to:</p> <ul style="list-style-type: none"> <li>• Create objects, object-groups and rules from a single panel</li> <li>• Filter on interfaces, source, destination or services</li> <li>• Policy query in the rule table for advanced filtering using multiple conditions</li> <li>• Show logs for a particular access rule in the real time log viewer</li> <li>• Select a rule and packet trace with a single click which will populate with appropriate packet attributes</li> <li>• Easily organize and move up and down in the table to change the order of access list entries</li> <li>• Expand and display elements in an object group</li> <li>• See attributes of a object or members of a group via tooltips</li> </ul>
High Availability and Scalability Wizard	The High Availability and Scalability Wizard is used to simplify configuration of Active/Active, Active/Standby failover and VPN Load balancing. The wizard also intelligently configures the peer device.

**Table 43** *New Features for ASA and PIX Version 7.2(1)/ASDM Version 5.2(1) (continued)*

Feature	Description
Syslog enhancements	Enhancements to the syslog features include: <ul style="list-style-type: none"> <li>• Syslog parsing to display source IP, destination IP, syslog ID, date and time into different columns</li> <li>• Integrated syslog references with explanations and recommended actions for each syslog with a single click</li> <li>• Syslog coloring based on severity level</li> <li>• A brief explanation of the syslogs as a tool tip in the log viewer</li> </ul>
NAT rules	The creation of NAT rules is simplified.
Object group support	There is now full ASDM support of network, service, protocol and ICMP-type object groups.
Named IP addresses	The ability to create a name to be associated with an IP Address now exists.
ASDM Assistant	The new ASDM Assistant provides task-oriented guidance to configuring features such as AAA server, logging filters, SSL VPN Client, and others features. You can also upload new guides.
Context management	Context management is improved, including context caching and better scalability.
Inspection maps	Predefined low, medium and high security settings simplify creation and management of inspection maps.

## New Features in Version 7.1

This section includes the following topics:

- [New Features in ASA 7.1\(2\)/ASDM 5.1\(2\), page 141](#)
- [New Features in ASA 7.1\(1\)/ASDM 5.1\(1\), page 141](#)

### New Features in ASA 7.1(2)/ASDM 5.1(2)

**Released: March 15, 2006**

There were no new features in ASA 7.1(2)/ASDM 5.1(2)

### New Features in ASA 7.1(1)/ASDM 5.1(1)

**Released: February 6, 2006**

[Table 21](#) lists the new features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1).

**Table 44** *New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1)*

Feature	Description
Platform Features	

**Table 44**      ***New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)***

Feature	Description
Support for the Content Security and Control (CSC) SSM	<p>The CSC SSM, an integral part of Cisco's Anti-X solution, delivers industry-leading threat protection and content control at the Internet edge providing comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering services. The CSC SSM services module helps businesses more effectively protect their networks, increase network availability, and increase employee productivity through the following key elements:</p> <ul style="list-style-type: none"> <li>• <b>Antivirus</b>—Market leading antivirus, from Trend Micro, shields your internal network resources from both known and unknown virus attacks, at the most effective point in your infrastructure, the Internet gateway. By cleaning your email and web traffic at the perimeter, it eliminates the need for resource intensive malware infection clean-ups and ensures business continuity.</li> <li>• <b>Anti-Spyware</b>—Blocks spyware from entering your network through web traffic (HTTP &amp; FTP) and email traffic. Frees-up IT support resources from costly spyware removal procedures and improves employee productivity by blocking spyware at the gateway.</li> <li>• <b>Anti-Spam</b>—Effective blocking of spam with very low false positives helps to restore the effectiveness of your email communications, so contact with customers, vendors, and partners continues uninterrupted.</li> <li>• <b>Anti-Phishing</b>—Identity theft protection guards against phishing attacks thereby preventing employees inadvertently disclosing company or personal details which could lead to financial loss.</li> <li>• <b>Automatic Updates from TrendLabs</b>—The solution is backed and supported by one of the largest teams of virus, spyware and spam experts in the industry working 24x7 to ensure that your solution is providing the most up to date protection – automatically.</li> <li>• <b>Central Administration</b>—Easy, set-and-forget administration through a remotely accessible web-console and automated updates reduces IT support costs.</li> <li>• <b>Real-time protection for Web access, Mail (SMTP &amp; POP3) and FTP (file transfer)</b>—Even if the company mail is already protected, many employees will access their own private web-mail from their company PCs or laptops introducing yet another entry point for internet borne threats. Similarly, employees may directly download programs or files which may be similarly contaminated. Real-time protection of all web traffic at the internet gateway greatly reduces this often over-looked point of vulnerability.</li> <li>• <b>Full URL filtering capability with categories, scheduling and cache</b>—URL filtering can be used to control employee internet usage by blocking access to inappropriate or non-work related websites improving employee productivity and limiting the risk of legal action being taken by employees exposed to offensive web content.</li> <li>• <b>Email Content Filtering</b>—Email filtering minimizes legal liability for offensive material transferred by email and enforces regulatory compliance, helping organizations meet the requirements of legislation such as GLB and the Data Protection Act.</li> </ul>

**General VPN Features**

**Table 44**      ***New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)***

Feature	Description
Cisco Secure Desktop	<p>Cisco Secure Desktop (CSD) is an optional Windows software package you can install on the ASA to validate the security of client computers requesting access to your SSL VPN, ensure they remain secure while they are connected, and remove all traces of the session after they disconnect.</p> <p>After a remote PC running Microsoft Windows connects to the ASA, CSD installs itself and uses the IP address and presence of specific files, registry keys, and certificates to identify the type of location from which the PC is connecting. Following user authentication, CSD uses optional criteria as conditions for granting access rights. These criteria include the operating system, antivirus software, antispware, and personal firewall running on the PC.</p> <p>To ensure security while a PC is connected to your network, the Secure Desktop, a CSD application that runs on Microsoft Windows XP and Windows 2000 clients, limits the operations available to the user during the session. For remote users with administrator privileges, Secure Desktop uses the 168-bit Triple Data Encryption Standard (3DES) to encrypt the data and files associated with or downloaded during an SSL VPN session. For remote users with lesser privileges, it uses the Rivest Cipher 4 (RC4) encryption algorithm. When the session closes, Secure Desktop overwrites and removes all data from the remote PC using the U.S. Department of Defense (DoD) security standard for securely deleting files. This cleanup ensures that cookies, browser history, temporary files, and downloaded content do not remain after a remote user logs out or an SSL VPN session times out. CSD also uninstalls itself from the client PC.</p> <p>Cache Cleaner, which wipes out the client cache when the session ends, supports Windows XP, Windows 2000, Windows 9x, Linux, and Apple Macintosh OS X clients.</p>
Customized Access Control Based on CSD Host Checking	<p>Adaptive security appliances with Cisco Secure Desktop installed can specify an alternative group policy. The ASA uses this attribute to limit access rights to remote CSD clients as follows:</p> <ul style="list-style-type: none"> <li>• Always use it if you set the VPN feature policy to “Use Failure Group-Policy.”</li> <li>• Use it if you set the VPN feature policy to “Use Success Group-Policy, if criteria match” and the criteria then fail to match.</li> </ul> <p>This attribute specifies the name of the alternative group policy to apply. Choose a group policy to differentiate access rights from those associated with the default group policy. The default value is DfltGrpPolicy.</p> <p><b>Note</b>    The ASA does not use this attribute if you set the VPN feature policy to “Always use Success Group-Policy.”</p>

**Table 44**      **New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)**

Feature	Description
SSL VPN Client	<p>SSL VPN client is a VPN tunneling technology that gives remote users the connectivity benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers. SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the ASA.</p> <p>To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the ASA in the browser, and the browser connects to that interface and displays the WebVPN login screen. If the user satisfies the login and authentication, and the ASA identifies the user as <i>requiring</i> the SVC, the ASA downloads the SVC to the remote computer. If the ASA identifies the user as having the <i>option</i> to use the SVC, the ASA downloads the SVC to the remote computer while presenting a link on the user screen to skip the SVC installation.</p> <p>After downloading, the SVC installs and configures itself. When the connection terminates, SVC either remains or uninstalls itself (depending on the configuration) from the remote computer.</p>
WebVPN Functions and Performance Optimizations	<p>This version enhances WebVPN performance and functions through the following components:</p> <ul style="list-style-type: none"> <li>• Flexible content transformation/rewriting that includes complex JavaScript, VBScript, and Java</li> <li>• Server-side and browser caching</li> <li>• Compression</li> <li>• Proxy bypass</li> <li>• Application Profile Customization Framework support</li> <li>• Application keep-alive and timeout handling</li> <li>• Support for logical (VLAN) interfaces</li> </ul>
Citrix Support for WebVPN	<p>WebVPN users can now use a connection to the ASA to access Citrix MetaFrame services. In this configuration, the ASA functions as the Citrix secure gateway. Therefore you must configure your Citrix Web Interface software to operate in a mode that does not use the Citrix secure gateway. Install an SSL certificate onto the ASA interface to which remote users use a fully qualified domain name (FQDN) to connect; this function does not work if you specify an IP address as the common name (CN) for the SSL certificate. The remote user attempts to use the FQDN to communicate with the ASA. The remote PC must be able to use DNS or an entry in the System32\drivers\etc\hosts file to resolve the FQDN. Finally, use the <b>functions</b> command to enable Citrix.</p>
PDA Support for WebVPN	<p>You can access WebVPN from your Pocket PC 2003 or Windows Mobile X. If you are a PDA user, this makes accessing your private network more convenient. This feature requires no configuration.</p>

**Table 44**      ***New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)***

<b>Feature</b>	<b>Description</b>
WebVPN Support of Character Encoding for CIFS Files	<p>WebVPN now supports optional character encoding of portal pages to ensure proper rendering of Common Internet File System files in the intended language. The character encoding supports the character sets identified on the following Web page, including Japanese Shift-JIS characters:</p> <p><a href="http://www.iana.org/assignments/character-sets">http://www.iana.org/assignments/character-sets</a></p> <p>Use the <b>character-encoding</b> command to specify the character set to encode in WebVPN portal pages to be delivered to remote users. By default, the encoding type set on the remote browser determines the character set for WebVPN portal pages.</p> <p>The character-encoding attribute is a global setting that, by default, all WebVPN portal pages inherit. However, you can use the <b>file-encoding</b> command to specify the encoding for WebVPN portal pages from specific CIFS servers. Thus, you can use different file-encoding values for CIFS servers that require different character encodings.</p> <p>The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the proper rendering of file names or directory paths, as well as pages, are an issue.</p> <p><b>Tip:</b> The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the <b>page style</b> command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, or enter the <b>no page style</b> command in webvpn customization command mode to remove the font family.</p>
Compression for WebVPN and SSL VPN Client Connections	<p>Compression can reduce the size of the transferring packets and increase the communication performance, especially for connections with bandwidth limitations, such as with dialup modems and handheld devices used for remote access.</p> <p>Compression is enabled by default, for both WebVPN and SVC connections. You can configure compression using ASDM or CLI commands.</p> <p>You can disable compression for all WebVPN or SVC connections with the <b>compression</b> command from global configuration mode.</p> <p>You can disable compression for a specific group or user for WebVPN connections with the <b>http-comp</b> command, or for SVC connections with the <b>svc compression</b> command, in the group policy or username webvpn modes.</p>
Active/Standby Stateful Failover for WebVPN and SVC Connections	<p>During a failover, WebVPN and SVC connections, as well as IPSec connections, are reestablished with the secondary, standby security appliance for uninterrupted service. Active/standby failover requires a one-to-one active/standby match for each connection.</p> <p>A security appliance configured for failover shares authentication information about WebVPN users with the standby security appliance. Therefore, after a failover, WebVPN users do not need to reauthenticate.</p> <p>For SVC connections, after a failover, the SVC reconnects automatically with the standby security appliance.</p>



**Table 44**      **New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)**

Feature	Description
WebVPN Customization	<p>You can customize the WebVPN page that users see when they connect to the security appliance, and you can customize the WebVPN home page on a per-user, per-group, or per-tunnel group basis. Users or groups see the custom WebVPN home page after the security appliance authenticates them.</p> <p>You can use Cascading Style Sheet (CSS) parameters. To easily customize, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.</p>
Auto Applet Download	To run a remote application over WebVPN, a user clicks Start Application Access on the WebVPN homepage to download and start a port-forwarding Java applet. To simplify application access and shorten start time, you can now configure WebVPN to automatically download this port-forwarding applet when the user first logs in to WebVPN.
<b>Authentication and Authorization VPN Features</b>	
Override Account Disabled	<p>You can configure the ASA to override an account-disabled indication from a AAA server and allow the user to log on anyway.</p> <p>We introduced the following command: <b>override account disabled</b>.</p>
LDAP Support	You can configure the security appliance to authenticate and authorize IPsec VPN users, SSL VPN clients, and WebVPN users to an LDAP directory server. During authentication, the security appliance acts as a client proxy to the LDAP server for the VPN user, and authenticates to the LDAP server in either plain text or using the Simple Authentication and Security Layer (SASL) protocol. The security appliance supports any LDAP V3 or V2 compliant directory server. It supports password management features only on the Sun Microsystems Java System Directory Server and the Microsoft Active Directory server.
Password Management	<p>You can configure the ASA to warn end users when their passwords are about to expire. When you configure this feature, the ASA notifies the remote user at login that the current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password. This command is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.</p> <p>Note that this command does not change the number of days before the password expires, but rather specifies the number of days before expiration that the ASA starts warning the user that the password is about to expire. The default value is 14 days.</p> <p>For LDAP server authentication only, you can specify a specific number of days before expiration to begin warning the user about the pending expiration.</p> <p>We introduced the following command: <b>password management</b>.</p>

**Table 44**      ***New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)***

Feature	Description
Single sign-on (SSO)	<p>Single sign-on (SSO) support lets WebVPN users enter a username and password only once to access multiple protected services and web servers. You can choose among the following methods to configure SSO:</p> <ul style="list-style-type: none"> <li>• Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder)—You typically would choose to implement SSO with SiteMinder if your Web site security infrastructure already incorporates SiteMinder.</li> <li>• HTTP Forms—A common and standard approach to SSO authentication that can also qualify as a AAA method. You can use it with other AAA servers such as RADIUS or LDAP servers.</li> <li>• SSO with Basic HTTP and NTLM Authentication—The simplest of the three SSO methods passes WebVPN login credentials for authentication through to internal servers using basic HTTP or NTLM authentication. This method does not require an external SSO server.</li> </ul>
<b>Tunnel Group and Group Policy VPN Features</b>	
WebVPN Tunnel Group Type	This version adds a WebVPN tunnel group, which lets you configure a tunnel group with WebVPN-specific attributes, including the authentication method to use, the WebVPN customization to apply to the user GUI, the DNS group to use, alternative group names (aliases), group URLs, the NBNS server to use for CIFS name resolution, and an alternative group policy to apply to CSD users to limit access rights to remote CSD clients.
Group-Based DNS Configuration for WebVPN	You can define a list of DNS servers under a group. The list of DNS servers available to a user depends on the group that the user is assigned to. You can specify the DNS server to use for a WebVPN tunnel group. The default value is DefaultDNS.
New Login Page Option for WebVPN Users	You can optionally configure WebVPN to display a user login page that offers the user the opportunity to select the tunnel group to use for login. If you configure this option, the login page displays an additional field offering a drop-down menu of groups from which to select. The user is authenticated against the selected group.
Group Alias and Group URL	<p>You can create one or more alternate names by which the user can refer to a tunnel group by specifying one or more group aliases. The group aliases that you specify here appear in the drop-down list on the user login page. Each group can have multiple aliases or no alias. If you want the actual name of the tunnel group to appear on this list, specify it as an alias. This feature is useful when the same group is known by several common names, such as “Devtest” and “QA”.</p> <p>Specifying a group URL eliminates the need for the user to select a group at login. When a user logs in, the ASA looks for the user incoming URL in the tunnel-group-policy table. If it finds the URL and if this feature is enabled, then the ASA automatically selects the appropriate server and presents the user with only the username and password fields in the login window. If the URL is disabled, the dropdown list of groups also appears, and the user must make the selection.</p> <p>You can configure multiple URLs (or no URLs) for a group. You can enable or disable each URL individually. You must use a separate specification (<b>group-url</b> command) for each URL. You must specify the entire URL, which can use either the HTTP or HTTPS protocol.</p> <p>You cannot associate the same URL with multiple groups. The ASA verifies the uniqueness of the URL before accepting the URL for a tunnel group.</p>
<b>ASDM Features</b>	

**Table 44**      ***New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)***

<b>Feature</b>	<b>Description</b>
Management and Monitoring Support for the CSC SSM	ASDM Version 5.1 delivers an industry-first solution that blends the simplicity of Trend Micro's HTML-based configuration panels with the ingenuity of ASDM. This helps ensure consistent policy enforcement, and simplifies the complete provisioning, configuration, and monitoring processes for the rich unified threat management functions offered by the CSC SSM. ASDM provides a complementing monitoring solution with a new CSC SSM homepage and new monitoring panels. Once a CSC SSM is installed, the main ASDM homepage is automatically updated to display a new CSC SSM panel, which provides a historic view into threats, e-mail viruses, live events, and vital module statistics such as last installed software/signature updates, system resources, and more. Within the monitoring section of ASDM, a rich set of analysis tools provide detailed visibility into threats, software updates, resource graphs, and more. The Live Security Event Monitor is a new troubleshooting and monitoring tool that provides real-time updates regarding scanned or blocked e-mail messages, identified viruses/worms, detected attacks, and more. It gives administrators the option to filter messages using regular-expression string matching, so specific attack types and messages can be focused on and analyzed in detail.
Syslog to Access Rule Correlation	This ASDM release introduces a new Syslog to Access Rule Correlation tool that greatly enhances day-to-day security management and troubleshooting activities. With this dynamic tool, security administrators can quickly resolve common configuration issues, along with most user and network connectivity problems. Users can select a syslog message within the Real-Time Syslog Viewer panel, and by simply clicking the Create button at the top of the panel, can invoke the access-control options for that specific syslog. Intelligent defaults help ensure that the configuration process is simple, which helps improve operational efficiency and response times for business-critical functions. The Syslog to Access Rule Correlation tool also offers an intuitive view into syslog messages invoked by user-configured access rules.
Customized Syslog Coloring	ASDM allows for rapid critical system message identification and convenient syslog monitoring by allowing the colored grouping of syslog messages according to syslog level. Users can select the default coloring options, or create their own unique colored syslog profiles for ease of identification.
ASDM and WebVPN interface	ASDM and WebVPN can now run on the same interface simultaneously.
ASDM Demo Mode	ASDM Demo Mode initial support.

## New Features in Version 7.0

This section includes the following topics:

- [New Features in ASA 7.0\(8\)/ASDM 5.0\(8\) and ASDM 5.0\(9\), page 149](#)
- [New Features in ASA 7.0\(7\)/ASDM 5.0\(7\), page 151](#)
- [New Features in ASA 7.0\(6\)/ASDM 5.0\(6\), page 151](#)
- [New Features in ASA 7.0\(5\)/ASDM 5.0\(5\), page 151](#)
- [New Features in ASA 7.0\(4\)/ASDM 5.0\(4\), page 153](#)
- [New Features in ASA 7.0\(2\)/ASDM 5.0\(2\), page 155](#)
- [New Features in ASA 7.0\(1\)/ASDM 5.0\(1\), page 155](#)

**Note**

There was no 7.0(3)/5.0(3) release.

## New Features in ASA 7.0(8)/ASDM 5.0(8) and ASDM 5.0(9)

**Released: June 2, 2008**

[Table 21](#) lists the new features for ASA and PIX Version 7.0(8)/ASDM Version 5.0(8)/5.0(9).

**Note**

ASDM 5.0(9) does not include any new features; it includes caveat fixes only.

**Table 45**      **New Features for ASA and PIX Version 7.0(8)/ASDM Version 5.0(8) and 5.0(9)**

Feature	Description
<b>Firewall Features</b>	
Ethertype ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules are retained, but no new ones need to be added. <i>Also available in Version 7.2(4) and 8.0(4).</i>
<b>Remote Access Features</b>	
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in use is not being eliminated from the pool, the connection is not affected. However, if the address in use is being eliminated from the pool, the connection is brought down. <i>Also available in Version 7.2(4) and 8.0(4).</i>
<b>Connection Features</b>	
<b>clear conn</b> Command	The <b>clear conn</b> command was added to remove connections. <i>Also available in Version 7.2(4) and 8.0(4).</i>
Fragment full reassembly	The <b>fragment</b> command was enhanced with the <b>reassemble full</b> keywords to enable full reassembly for fragments that are routed through the device. Fragments that terminate at the device are always fully reassembled. <i>Also available in Version 7.2(4) and 8.0(4).</i>
<b>Troubleshooting and Monitoring Features</b>	
<b>capture</b> command Enhancement	The <b>capture type asp-drop drop_code</b> command now accepts <b>all</b> as the <i>drop_code</i> , so you can now capture all packets that the ASA drops, including those dropped due to security checks. <i>Also available in Version 7.2(4) and 8.0(4).</i>
<b>show asp drop</b> Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the <b>clear asp drop</b> command). It also displays the drop reason keywords next to the description, so you can easily use the <b>capture asp-drop</b> command using the keyword. <i>Also available in Version 7.2(4) and 8.0(4).</i>
<b>clear asp table</b> Command	Added the <b>clear asp table</b> command to clear the hits output by the <b>show asp table</b> commands. <i>Also available in Version 7.2(4) and 8.0(4).</i>

**Table 45**      **New Features for ASA and PIX Version 7.0(8)/ASDM Version 5.0(8) and 5.0(9) (continued)**

Feature	Description
<b>show asp table classify hits</b> Command Enhancement	<p>The <b>hits</b> option was added to the <b>show asp table classify</b> command, showing the timestamp indicating the last time the asp table counters were cleared. It also shows rules with hits values not equal to zero. This permits users to quickly see what rules are being hit, especially since a simple configuration may end up with hundreds of entries in the <b>show asp table classify</b> command.</p> <p><i>Also available in Version 7.2(4) and 8.0(4).</i></p>
<b>show perfmon</b> Command	<p>Added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Attempts, TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept.</p> <p><i>Also available in Version 7.2(4) and 8.0(4).</i></p>
<b>memory tracking</b> Commands	<p>The following new commands are introduced in this release:</p> <ul style="list-style-type: none"> <li>• <b>memory tracking enable</b>—This command enables the tracking of heap memory requests.</li> <li>• <b>no memory tracking enable</b>—This command disables tracking of heap memory requests, cleans up all currently gathered information, and returns all heap memory used by the tool itself to the system.</li> <li>• <b>clear memory tracking</b>—This command clears out all currently gathered information but continues to track further memory requests.</li> <li>• <b>show memory tracking</b>—This command shows currently allocated memory tracked by the tool, broken down by the topmost caller function address.</li> <li>• <b>show memory tracking address</b>—This command shows currently allocated memory broken down by each individual piece of memory. The output lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool.</li> <li>• <b>show memory tracking dump</b>—This command shows the size, location, partial callstack, and a memory dump of the given memory address.</li> <li>• <b>show memory tracking detail</b>—This command shows various internal details to be used in gaining insight into the internal behavior of the tool.</li> </ul> <p><i>Also available in Version 7.2(4) and 8.0(4).</i></p>
<b>Failover Features</b>	
<b>failover timeout</b> Command	<p>The <b>failover timeout</b> command no longer requires a failover license for use with the static nailed feature.</p> <p><i>Also available in Version 7.2(4) and 8.0(4).</i></p>
<b>Usability Features</b>	
<b>show access-list</b> Output	<p>Expanded access list output is indented to make it easier to read.</p> <p><i>Also available in Version 7.2(4) and 8.0(4).</i></p>
<b>show arp</b> Output	<p>In transparent firewall mode, you might need to know whether an ARP entry is statically configured or dynamically learned. ARP inspection drops ARP replies from a legitimate host if a dynamic ARP entry has already been learned. ARP inspection only works with static ARP entries. The <b>show arp</b> command now shows each entry with its age if it is dynamic, or no age if it is static.</p> <p>See <b>Monitoring &gt; Interfaces &gt; ARP Table</b>.</p> <p><i>Also available in Version 7.2(4) and 8.0(4).</i></p>

**Table 45** *New Features for ASA and PIX Version 7.0(8)/ASDM Version 5.0(8) and 5.0(9) (continued)*

Feature	Description
<b>show conn</b> Command	The syntax was simplified to use source and destination concepts instead of “local” and “foreign.” In the new syntax, the source address is the first address entered and the destination is the second address. The old syntax used keywords like foreign and port to determine the destination address and port.
<b>ASDM Features</b>	
Support for fragment option	ASDM now supports a fragment option to reassemble packets routed through ASDM. To configure this feature, see <b>Configuration &gt; Properties &gt; Advanced &gt; Fragment</b> .

## New Features in ASA 7.0(7)/ASDM 5.0(7)

Released: July 9, 2007

[Table 21](#) lists the new features for ASA and PIX Version 7.0(7)/ASDM Version 5.0(7).

**Table 46** *New Features for ASA and PIX Version 7.0(7)/ASDM Version 5.0(7)*

Feature	Description
<b>Module Features</b>	
Added Dataplane Keepalive Mechanism	You can now configure the ASA so that a failover will not occur if the AIP SSM is upgraded. In previous releases when two ASAs with AIP SSMs are configured in failover and the AIP SSM software is updated, the ASA triggers a failover, because the AIP SSM needs to reboot or restart for the software update to take effect. <i>Also available in Version 7.2(3) and 8.0(3)</i>

## New Features in ASA 7.0(6)/ASDM 5.0(6)

Released: August 22, 2006

There were no new features in ASA 7.0(6)/ASDM 5.0(6)

## New Features in ASA 7.0(5)/ASDM 5.0(5)

Released: April 14, 2006

Table 21 lists the new features for ASA and PIX Version 7.0(5)/ASDM Version 5.0(5).

**Table 47**      **New Features for ASA and PIX Version 7.0(5)/ASDM Version 5.0(5)**

Feature	Description
<b>Application Inspection Features</b>	
Command to Control DNS Guard	<p>You can now control the DNS guard function. In releases prior to 7.0(5), the DNS guard functions are always enabled regardless of the configuration of DNS inspection:</p> <ul style="list-style-type: none"> <li>• Stateful tracking of the DNS response with DNS request to match the ID</li> <li>• Tearing down the DNS connection when all pending requests are responded</li> </ul> <p>This command is effective only on interfaces with DNS inspection disabled (<b>no inspect dns</b>). When DNS inspection is enabled, the DNS guard function is always performed.</p> <p>We introduced the following command: <b>dns guard</b>.</p>
Enhanced IPSEC Inspection	<p>The ability to open specific pinholes for ESP flows based on existence of an IKE flow is provided by the enhanced IPsec inspect feature. This feature can be configured within the MPF infrastructure along with other inspects. The idle-timeout on the resulting ESP flows is statically set at 10 minutes. There is no maximum limit on number of ESP flows that can be allowed.</p> <p>We introduced the following command: <b>inspect ipsec-pass-thru</b>.</p>
<b>Firewall Features</b>	
Command to Disable RST for Denied TCP Packets	<p>When a TCP packet is denied, the adaptive security appliance always sends a reset when the packet is going from a high security to a low security interface. The <b>service resetinbound</b> command is used to enable or disable sending resets when a TCP packet is denied when going from a low security to a high security interface. The <b>service resetinbound</b> command is introduced to control sending RESETs when a packet is denied when going from a high security to a low security interface. The existing <b>service resetinbound</b> command is enhanced to take an additional interface option.</p> <p>We introduced the following commands: <b>service resetoutbound</b>, <b>service resetinbound</b>.</p>
<b>Platform Features</b>	
Increased Connections and VLANs	<p>The maximum connections and VLANs is increased to the following numbers.</p> <ul style="list-style-type: none"> <li>• ASA5510 base license conns 32000-&gt;50000 vlans 0-&gt;10</li> <li>• ASA5510 plus license conns 64000-&gt;130000 vlans 10-&gt;25</li> <li>• ASA5520 conns 130000-&gt;280000 vlans 25-&gt;100</li> <li>• ASA5540 conns 280000-&gt;400000 vlans 100-&gt;200</li> </ul>
<b>Management Features</b>	

**Table 47** *New Features for ASA and PIX Version 7.0(5)/ASDM Version 5.0(5) (continued)*

Feature	Description
Password Increased in Local Database	Username and enable password length limits increased from 16 to 32 in the LOCAL database.
Enhanced <b>show interface</b> and <b>show traffic</b> Commands	<p>The traffic statistics displayed in both the <b>show interface</b> and <b>show traffic</b> commands now support 1 minute rate and 5 minute rate for input, output and drop. The rate is calculated as the delta between the last two sampling points. For a 1 minute rate and a 5 minute rate, a 1 minute timer and a 5 minute timer are run constantly for the rates respectively. An example of the new display follows:</p> <pre> 1 minute input rate 128 pkts/sec,  15600 bytes/sec 1 minute output rate 118 pkts/sec,  13646 bytes/sec 1 minute drop rate 12 pkts/sec 5 minute input rate 112 pkts/sec,  13504 bytes/sec 5 minute output rate 101 pkts/sec,  12104 bytes/sec 5 minute drop rate 4 pkts/sec </pre>

## New Features in ASA 7.0(4)/ASDM 5.0(4)

Released: October 15, 2005

[Table 21](#) lists the new features for ASA and PIX Version 7.0(4)/ASDM Version 5.0(4).

**Table 48** *New Features for ASA and PIX Version 7.0(4)/ASDM Version 5.0(4)*

Feature	Description
<b>Platform Features</b>	
Support for the 4GE SSM	The 4GE Security Services Module (SSM) is an optional I/O card for the adaptive security appliance. The 4GE SSM expands the total number of ports available on the security appliance, providing four additional ports with Ethernet (RJ-45) or SFP (fiber optic) connections.
<b>VPN Features</b>	
WebVPN Capture Feature	The WebVPN capture feature lets you log information about websites that do not display properly over a WebVPN connection. You can enable the WebVPN capture feature with the <b>capture</b> command, but note that it has an adverse affect on the performance of the security appliance. So, be sure to disable this feature after you have captured the information that you need for troubleshooting.
Auto Update Over a VPN Tunnel	<p>With this release, the <b>auto-update server</b> command has a new <b>source interface</b> argument that lets you specify an interface, such as a VPN tunnel used for management access and specified by the <b>management-access</b> command:</p> <pre> <b>auto-update server url [source interface] [verify-certificate]</b> </pre>



**Table 48**      **New Features for ASA and PIX Version 7.0(4)/ASDM Version 5.0(4) (continued)**

Feature	Description
HTTP proxy applet	<p>The HTTP proxy is an Internet Proxy, that supports both HTTP and HTTPS connections. The HTTP proxy code modifies the browser proxy configuration dynamically to redirect all browser HTTP/S requests to the new proxy configuration. This allows the Java Applet to take over as the proxy for the browser.</p> <p>HTTP Proxy can be used in conjunction with the Port Forwarding (Application Access) feature or by itself.</p> <p><b>Note</b>    The HTTP proxy feature only works when using Internet Explorer.</p> <p>On some of the older computers, running Windows XP, the RunOnce Reg-Key is not available, causing the Port Forwarding HTTP-Proxy feature to fail when attempting to modify Proxy settings on Internet Explorer.</p> <p>You can manually change the registry. Complete the following steps to change the registry manually:</p> <ol style="list-style-type: none"> <li>Click <b>Start   Run</b>.</li> <li>Type <b>regedit</b> in the open text box, and click <b>OK</b>.</li> <li>Open this folder: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\</li> <li>Right click inside the CurrentVersion and select <b>New   Key</b>.</li> <li>Name the new key <b>RunOnce</b>.</li> <li>Click <b>OK</b>.</li> </ol> <p>To configure file access and file browsing, MAPI Proxy, HTTP Proxy, and URL entry over WebVPN for this user or group policy, use the <b>functions</b> command in WebVPN mode.</p>
IPSec VPN: Add support for cascading ACLs	<p>Cascading ACLs involves the insertion of deny ACEs to bypass evaluation against an ACL and resume evaluation against a subsequent ACL in the crypto map set. Because you can associate each crypto map with different IPSec settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security. The sequence number assigned to the crypto ACL determines its position in the evaluation sequence within the crypto map set.</p>
<b>Troubleshooting and Monitoring Features</b>	
Crashinfo Enhancement	<p>Output from the <b>crashinfo</b> command might contain sensitive information that is inappropriate for viewing by all users connected to the ASA. The new <b>crashinfo console disable</b> command lets you suppress the output from displaying on the console.</p>
Rate limiting of Syslog messages	<p>The logging rate limit enables you to limit the rate at which system log messages are generated. You can limit the number of system messages that are generated during a specified time interval.</p> <p>You can limit the message generation rate for all messages, a single message ID, a range of message IDs, or all messages with a particular severity level. To limit the rate at which system log messages are generated, use the <b>logging rate-limit</b> command.</p>
<b>Firewall Features</b>	
Connection timeout using Modular Policy Framework	<p>The new <b>set connection timeout</b> command lets you configure the timeout period, after which an idle TCP connection is disconnected.</p>

**Table 48**      ***New Features for ASA and PIX Version 7.0(4)/ASDM Version 5.0(4) (continued)***

Feature	Description
Downloadable ACL Enhancements	<p>A new feature has been added to ensure that downloadable ACL requests sent to a RADIUS server come from a valid source through the Message-Authenticator attribute.</p> <p>Upon receipt of a RADIUS authentication request that has a username attribute containing the name of a downloadable ACL, Cisco Secure ACS authenticates the request by checking the Message-Authenticator attribute. The presence of the Message-Authenticator attribute prevents malicious use of a downloadable ACL name to gain unauthorized network access. The Message-Authenticator attribute and its use are defined in RFC 2869, RADIUS Extensions, available at <a href="http://www.ietf.org">http://www.ietf.org</a>.</p>
Converting Wildcards to Network Mask in Downloadable ACL	<p>Some Cisco products, such as the VPN 3000 concentrator and Cisco IOS routers, require you to configure downloadable ACLs with wildcards instead of network masks. The Cisco ASA 5500 adaptive security appliance, on the other hand, requires you to configure downloadable ACLs with network masks. This new feature allows the ASA to convert a wildcard to a netmask internally. Translation of wildcard netmask expressions means that downloadable ACLs written for Cisco VPN 3000 series concentrators can be used by the ASA without altering the configuration of the downloadable ACLs on the RADIUS server.</p> <p>You can configure ACL netmask conversion on a per-server basis, using the <b>acl-netmask-convert</b> command, available in the AAA-server configuration mode.</p>
<b>Application Inspection Features</b>	
Support GTP Load Balancing Across GSNs	<p>If the ASA performs GTP inspection, by default the ASA drops GTP responses from GSNs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs to provide efficiency and scalability of GPRS. You can enable support for GSN pooling by using the <b>permit response</b> command. This command configures the ASA to allow responses from any of a designated set of GSNs, regardless of the GSN to which a GTP request was sent.</p>

**Note**

There was no 7.0(3)/5.0(3) release.

## New Features in ASA 7.0(2)/ASDM 5.0(2)

**Released: July 22, 2005**

There were no new features in ASA 7.0(2)/ASDM 5.0(2)

## New Features in ASA 7.0(1)/ASDM 5.0(1)

**Released: May 31, 2005**

Table 21 lists the new features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1).

**Table 49**      **New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1)**

Feature	Description
<b>Platform Features</b>	
Support for the ASA 5500 series	Support for the ASA 5500 series was introduced, including support for the following models: ASA 5510, ASA 5520, and ASA 5540.
<b>Firewall Features</b>	
Transparent Firewall (Layer 2 Firewall)	<p>This feature has the ability to deploy the ASA in a secure bridging mode, similar to a Layer 2 device, to provide rich Layer 2 – 7 firewall security services for the protected network. This enables businesses to deploy this ASA into existing network environments without requiring readdressing of the network. While the ASA can be completely “invisible” to devices on both sides of a protected network, administrators can manage it via a dedicated IP address (which can be hosted on a separate interface). Administrators have the ability to specify non-IP (EtherType) ACLs, in addition to standard ACLs, for access control over Layer 2 devices and protocols.</p> <p>We introduced the following commands: <b>arp-inspection</b>, <b>firewall</b>, <b>mac-address-table</b>, and <b>mac-learn</b>.</p>
Security Contexts (Virtual Firewall)	<p>This feature introduces the ability to create multiple security contexts (virtual firewalls) within a single appliance, with each context having its own set of security policies, logical interfaces, and administrative domain. This provides businesses a convenient way of consolidating multiple firewalls into a single physical appliance, yet retaining the ability to manage each of these virtual instances separately. These capabilities are only available on ASA with either unrestricted (UR) or failover (FO) licenses. This is a licensed feature, with multiple tiers of supported security contexts (2, 5, 10, 20, and 50).</p> <p>We introduced the following commands: <b>admin-context</b>, <b>context</b> (and context subcommands), <b>changeto</b>, and <b>mode</b>.</p>
Outbound ACLs and	This feature gives administrators improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs (building on top of our existing inbound ACL support). Using these new capabilities, administrators can now apply access controls as traffic enters an interface or exits an interface. Time-based access control lists provide administrators greater control over resource usage by defining when certain ACL entries are active. New commands allow administrators to define time ranges, and then apply these time ranges to specific ACLs.
Time-based ACLs	The existing versatile <b>access-list</b> global configuration command was extended with the <b>time-range</b> command to specify a time-based policy defined using the <b>time-range</b> global configuration command. Additionally, the <b>access-group</b> global configuration command supports the <b>out</b> keyword to configure an outbound ACL.
Enabling/Disabling of ACL Entries	This feature provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs, without the need to remove and replace ACL entries.
EtherType Access Control	This feature includes very powerful support for performing packet filtering and logging based on the EtherType of the packets. When operating as a transparent firewall, this provides tremendous flexibility for permitting or denying non-IP protocols.

**Table 49**      ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Modular Policy Framework	<p>This feature introduces a highly flexible and extensible next-generation modular policy framework. It enables the construction of flow-based policies that identify specific flows based on administrator-defined conditions, and then apply a set of services to that flow (such as firewall/inspection policies, VPN policies, QoS policies, and more). This provides significantly improved granular control over traffic flows, and the services performed on them. This new framework also enables inspection engines to have flow-specific settings (which were global in previous releases).</p> <p>We introduced the following commands: <b>class-map</b>, <b>policy-map</b>, and <b>service-policy</b>.</p>
TCP Security Engine	<p>This feature introduces several new foundational capabilities to assist in detecting protocol and application layer attacks. TCP stream reassembly helps detect attacks that are spread across a series of packets by reassembling packets into a full packet stream and performing analysis of the stream. TCP traffic normalization provides additional techniques to detect attacks including advanced flag and option checking, detection of data tampering in retransmitted packets, TCP packet checksum verification, and more.</p> <p>You can configure the extensive TCP security policy using the <b>set connection advanced-options</b> in global configuration command and <b>tcp-map</b> global configuration command.</p>
Outbound Low Latency Queuing (LLQ) and Policing	<p>This feature supports applications with demanding quality of service (QoS) requirements through support of Low Latency Queuing (LLQ) and Traffic Policing – supporting the ability to have an end-to-end network QoS policy. When enabled, each interface maintains two queues for outbound traffic – one for latency-sensitive traffic (such as voice or market-data), and one for latency-tolerant traffic (such as file transfers). Queue performance can be optimized through a series of configuration parameters.</p> <p>The QoS functionality is managed using the following commands: <b>police</b>, <b>priority</b>, <b>priority-queue</b>, <b>queue-limit</b>, and <b>tx-ring-limit</b>.</p>
<b>Application Inspection Features</b>	
Advanced HTTP Inspection Engine	<p>This feature introduces deep analysis of web traffic, enabling granular control over HTTP sessions for improved protection from a wide range of web-based attacks. In addition, this new HTTP inspection engine allows administrative control over instant messaging applications, peer-to-peer file sharing applications, and applications that attempt to tunnel over port 80 or any port used for HTTP transactions. Capabilities provided include RFC compliance enforcement, HTTP command authorization and enforcement, response validation, Multipurpose Internet Mail Extension (MIME) type validation and content control, Uniform Resource Identifier (URI) length enforcement, and more.</p> <p>A user can define the advanced HTTP Inspection policy using the <b>http-map</b> global configuration command and then apply it to the <b>inspect http</b> configuration mode command that was extended to support the specification of a map name.</p>
FTP Inspection Engine	<p>This feature includes the FTP inspection engine which provides new command filtering support. Building upon the FTP security services previously supported, such as protocol anomaly detection, protocol state tracking, NAT/PAT support, and dynamic port opening, Version 7.0 gives administrators granular control over the usage of 9 different FTP commands, enforcing operations that users/groups can perform in FTP sessions. Version 7.0 also introduces FTP server cloaking capabilities, hiding the type and version of the FTP server from those who access it through ASA.</p>

**Table 49**      **New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)**

Feature	Description
ESMTP Inspection Engine	<p>This feature builds on the SMTP (RFC 821) feature with the addition of support for the SMTP (ESMTP) protocol, featuring a variety of commands defined in RFC 1869. Supported commands include <b>AUTH</b>, <b>DATA</b>, <b>EHLO</b>, <b>ETRN</b>, <b>HELO</b>, <b>HELP</b>, <b>MAIL</b>, <b>NOOP</b>, <b>QUIT</b>, <b>RCPT</b>, <b>RSET</b>, <b>SAML</b>, <b>SEND</b>, <b>SOML</b>, and <b>VERFY</b> (all other commands are automatically blocked to provide an additional level of security).</p> <p>The <b>inspect esmtp</b> global configuration command provides inspection services for SMTP and ESMTP traffic.</p>
SunRPC / NIS+ inspection engine	<p>The SunRPC inspection engine provides better support for NIS+ and SunRPC services. Specific enhancements include support for all three versions of the lookup service - Portmapper v2 and RPCBind v3 and v4.</p> <p>Use the <b>inspect sunrpc</b> and the <b>sunrpc-server</b> global configuration commands to configure the SunRPC / NIS+ inspection Engine.</p>
ICMP Inspection Engine	<p>This feature introduces an ICMP inspection engine. This engine enables secure usage of ICMP, by providing stateful tracking for ICMP connections, matching echo requests with replies. Additional controls are available for ICMP error messages, which are only permitted for established connections. This release introduces the ability to NAT ICMP error messages.</p> <p>Use the <b>inspect icmp</b> and the <b>inspect icmp error</b> commands to configure the ICMP inspection engine.</p>
GTP Inspection Engine for Mobile Wireless Environments	<p>This feature introduces a new inspection engine for securing 3G Mobile Wireless environments that provide packet switched data services using the GPRS Tunneling Protocol (GTP). These new advanced GTP inspection services permit mobile service providers secure interaction with roaming partners and provide mobile administrators robust filtering capabilities based on GTP specific parameters such as IMSI prefixes, APN values and more. This is a licensed feature.</p> <p>The <b>inspect gtp</b> command in the policy-map configuration mode and the <b>gtp-map</b> global configuration commands are new features introduced in Version 7.0. For more information on GTP and detailed instructions for configuring your GTP inspection policy, see the “Managing GTP Inspection” section in the <i>Cisco ASA 5500 Series Configuration Guide using the CLI</i>. You may need to install a GTP activation key using the <b>activation-key exec</b> command.</p>
H.323 Inspection Engine	<p>The H.323 inspection engine adds support for the T.38 protocol, an ITU standard that enables the secure transmission of Fax over IP (FoIP). Both real-time and store-and-forward FAX methods are supported. The H.323 inspection engine supports Gatekeeper Routed Call Signaling (GKRCS) in addition to the Direct Call Signaling (DCS) method currently supported. GKRCS support, based on the ITU standard, now allows the ASA to handle call signaling messages exchanged directly between H.323 Gatekeepers.</p>
H.323 Version 3 and 4 Support	<p>This release supports NAT and PAT for H.323 versions 3 and 4 messages, and in particular, the H.323 v3 feature Multiple Calls on One Call Signaling Channel.</p>
SIP Inspection Engine	<p>This feature adds support for Session Initiation Protocol (SIP)-based instant messaging clients, such as Microsoft Windows Messenger. Enhancements include support for features described by RFC 3428 and RFC 3265.</p>
Support for Instant Messaging Using SIP	<p>Fixup SIP now supports the Instant Messaging (IM) Chat feature on Windows XP using Windows Messenger RTC client version 4.7.0105 only.</p>
Configurable SIP UDP Inspection Engine	<p>This provides a CLI-enabled solution for non-Session Information Protocol (SIP) packets to pass through the ASA instead of being dropped when they use a SIP UDP port.</p>

**Table 49**      ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
MGCP Inspection Engine	<p>This feature includes an MGCP inspection engine that supports NAT and PAT for the MGCP protocol. This ensures seamless security integration in distributed call processing environments that include MGCP Version 0.1 or 1.0 as the VoIP protocol.</p> <p>The <b>inspect mgcp</b> command in the policy-map configuration mode and the <b>mgcp-map</b> global <b>configuration</b> command enables the user to configure MGCP inspection policy.</p>
RTSP Inspection Engine	<p>This feature introduces NAT support for the Real Time Streaming Protocol (RTSP), which allows streaming applications such as Cisco IP/TV, Apple Quicktime, and RealNetworks RealPlayer to operate transparently across NAT boundaries.</p>
SNMP Inspection Engine	<p>Similar to other new inspection engines, the <b>inspect snmp</b> command in policy-map configuration mode and the <b>snmp-map</b> global configuration command enables the user to configure an SNMP inspection policy.</p>
Port Address Translation (PAT) for H.323 and SIP Inspection Engines	<p>This release enhances support for the existing H.323 and SIP inspection engines by adding support for Port Address Translation (PAT). Adding support for PAT with H.323 and SIP enables our customers to expand their network address space using a single global address.</p>
PAT for Skinny	<p>This feature allows Cisco IP Phones to communicate with Cisco CallManager across the ASA when it is configured with PAT. This is particularly important in a remote access environment where Skinny IP phones behind a ASA talk to the CallManager at the corporate site through a VPN.</p>
ILS Inspection Engine	<p>This feature provides an Internet Locator Service (ILS) fixup to support NAT for ILS and Lightweight Directory Access Protocol (LDAP). Also, with the addition of this fixup, the ASA supports H.323 session establishment by Microsoft NetMeeting. Microsoft NetMeeting, SiteServer, and Active Directory products leverage ILS, which is a directory service, to provide registration and location of endpoints. ILS supports the LDAP protocol and is LDAPv2 compliant.</p>
Configurable RAS Inspection Engine	<p>This feature includes an option to turn off the H.323 RAS (Registration, Admission, and Status) fixup and displays this option, when set, in the configuration. This enables customers to turn off the RAS fixup if they do not have any RAS traffic, they do not want their RAS messages to be inspected, or if they have other applications that utilize the UDP ports 1718 and 1719.</p>
CTIQBE Inspection Engine	<p>Known also as TAPI/JTAPI Fixup, this feature incorporates a Computer Telephony Interface Quick Buffer Encoding (CTIQBE) protocol inspection module that supports NAT, PAT, and bi-directional NAT. This enables Cisco IP SoftPhone &amp; other Cisco TAPI/JTAPI applications to work and communicate successfully with Cisco CallManager for call setup and voice traffic across the ASA.</p> <p>This release supports the <b>inspect ctiqbe 2748</b> command.</p>
MGCP Inspection Engine	<p>This release adds support for Media Gateway Control Protocol (MGCP) 1.0, enabling messages between Call Agents and VoIP media gateways to pass through the ASA in a secure manner.</p> <p>See the <b>inspect mgcp</b> command.</p>
Ability to Configure TFTP Inspection Engine	<p>Ability to configure TFTP inspection engine inspects the TFTP protocol and dynamically creates connection and xlate, if necessary, to permit file transfer between a TFTP client and server. Specifically, the fixup inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).</p> <p><b>Note</b>    TFTP Fixup is enabled by default. TFTP Fixup must be enabled if static PAT is used to redirect TFTP traffics.</p>

**Table 49**      **New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)**

Feature	Description
<b>Filtering Features</b>	
Improved URL Filtering Performance	<p>This feature significantly increases the number of concurrent URLs that can be processed by improving the communications channel between the ASA and the Websense servers.</p> <p>The existing <b>url-server</b> global configuration command now supports the <b>connections</b> keyword to specify the number of TCP connections in the pool that is used.</p>
URL Filtering Enhancements	<p>This release supports N2H2 URL filtering services for URLs up to 1159 bytes.</p> <p>For Websense, long URL filtering is supported for URLs up to 4096 bytes in length.</p> <p>Additionally, this release provides a configuration option to buffer the response from a web server if its response is faster than the response from either an N2H2 or Websense filtering service server. This prevents the web server's response from being loaded twice.</p>
<b>IPSec VPN Features</b>	
Incomplete Crypto Map Enhancements	<p>Every static crypto map must define an access list and an IPSec peer. If either is missing, the crypto map is considered incomplete and a warning message is printed. Traffic that has not been matched to an complete crypto map is skipped, and the next entry is tried. Failover hello packets are exempt from the incomplete crypto map check.</p>
Spoke-to-Spoke VPN Support	<p>This feature improves support for spoke-to-spoke (and client-to-client) VPN communications, by providing the ability for encrypted traffic to enter and leave the same interface. Furthermore, split-tunnel remote access connections can now be terminated on the outside interface for the ASA, allowing Internet-destined traffic from remote access user VPN tunnels to leave on the same interface as it arrived (after firewall rules have been applied).</p> <p>The <b>same-security-traffic</b> command permits traffic to enter and exit the same interface when used with the <b>intra-interface</b> keyword enabling spoke-to-spoke VPN support.</p>
OSPF Dynamic Routing over VPN	<p>Support for OSPF has been extended to support neighbors across an IPSec VPN tunnel. This allows the ASA to support dynamic routing updates across a VPN tunnel to other OSPF peers. OSPF hellos are unicast and encrypted for transport down the tunnel to an identified neighbor in an RFC- compliant manner.</p> <p>The <b>ospf network point-to-point non-broadcast</b> command in interface configuration mode extends comprehensive OSPF dynamic routing services to support neighbors across IPSec VPN tunnels, providing improved network reliability for VPN connected networks.</p>
Remote Management Enhancements	<p>This feature enables administrators to remotely manage firewalls over a VPN tunnel using the inside interface IP address of the remote ASA. In fact, administrators can define any ASA interface for management-access. This feature supports ASDM, SSH, Telnet, SNMP, and so on, that requires a dynamic IP address. This feature significantly benefits broadband environments.</p>
X.509 Certificate Support	<p>Support for X.509 certificates has been significantly improved in the ASA, adding support for n-tier certificate chaining (for environments with a multi-level certification authority hierarchy), manual enrollment (for environments with offline certificate authorities), and support for 4096-bit RSA keys. Version 7.0 also includes support for the new certificate authority introduced in Cisco IOS software, a lightweight X.509 certificate authority designed to simplify roll-out of PKI-enabled site-to-site VPN environments.</p>

**Table 49**      **New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)**

Feature	Description
Easy VPN Server	<p>This release supports Cisco Easy VPN server. Cisco Easy VPN server is designed to function seamlessly with existing VPN headend configured to support Cisco VPN client and to minimize the administrative overhead for the client by centralizing VPN configuration at the Cisco Easy VPN server. Examples of Cisco Easy VPN server products include the Cisco VPN client v3.x and greater and the Cisco VPN 3002 Hardware client.</p> <p><b>Note</b>    The ASA already acts as a central site VPN device and supports the termination of remote access VPN clients.</p>
Easy VPN Server Load Balancing Support	The ASA 5500 ASA can participate in cluster-based concentrator load balancing. It supports VPN 3000 series concentrator load balancing with automatic redirection to the least utilized concentrator.
Dynamic Downloading of Backup Easy VPN Server Information	<p>Support for downloading a list of backup concentrators defined on the headend.</p> <p>This feature supports the <b>vpngroup group_name backup-server {{ip1 [ip2... ip10]}   clear-client-cfg}</b> commands.</p>
Easy VPN Internet Access Policy	<p>The ASA changes the behavior of a ASA used as an Easy VPN remote device in regard to Internet access policy for users on the protected network. The new behavior occurs when split tunneling is enabled on the Easy VPN server. Split tunneling is a feature that allows users connected through the ASA to access the Internet in a clear text session, without using a VPN tunnel.</p> <p>The ASA used as an Easy VPN remote device downloads the split tunneling policy and saves it in its local Flash memory when it first connects to the Easy VPN server. If the policy enables split tunneling, users connected to the network protected by the ASA can connect to the Internet regardless of the status of the VPN tunnel to the Easy VPN server.</p>
Verify Certificate Distinguished Name	This feature enables the adaptive security appliances acting as either a VPN peer for site to site, or as the Easy VPN server in remote access deployments to validate matching of a certificate to an administrator specified criteria.
Easy VPN Web Interface for Manual Tunnel Control User Authentication and Tunnel Status	With the introduction of the User-Level Authentication and Secure Unit Authentication, features the ASA delivers the ability to enter the credentials, connect/dis-connect the tunnel and monitor the connection using new web pages served to users when attempting access to the VPN tunnel or unprotected networks through the ASA. This is only applicable to the Easy VPN server feature.
User-Level Authentication	<p>Support for individually authenticating clients (IP address based) on the inside network of the ASA. Both static and One Time Password (OTP) authentication mechanisms are supported. This is done through a web-based interface.</p> <p>This feature adds support to the <b>vpn-group-policy</b> command.</p>
Secure Unit Authentication	This feature provides the ability to use dynamically generated authentication credentials to authenticate the Easy VPN remote (VPN Hardware client) device.
Flexible Easy VPN Management Solutions	Managing the ASA using the outside interface will not require the traffic to flow over the VPN tunnel. You will have the flexibility to require all NMS traffic to flow over the tunnel or fine tune this policy.
VPN Client Security Posture Enforcement	<p>This feature introduces the ability to perform VPN client security posture checks when a VPN connection is initiated. Capabilities include enforcing usage of authorized host-based security products (such as the Cisco Security Agent) and verifying its version number, policies, and status (enabled/disabled).</p> <p>To set personal firewall policies that the security appliance pushes to the VPN client during IKE tunnel negotiation, use the <b>client-firewall</b> command in group-policy configuration mode.</p>



**Table 49**      ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
VPN Client Update	To configure and change client update parameters, use the <b>client-update</b> command in tunnel-group ipsec-attributes configuration mode.
VPN Client Blocking by Operating System and Type	<p>This feature adds the ability to restrict the different types of VPN clients (software client, router, VPN 3002, and PIX) that are allowed to connect based on type of client, operating system version installed, and VPN client software version. When non-compliant users attempt to connect, they can be directed to a group that specifically allows connections from non-compliant users.</p> <p>To configure rules that limit the remote access client types and versions that can connect via IPSec through the ASA, use the <b>client-access-rule</b> command in group-policy configuration mode.</p>
Movian VPN Client Support	<p>This feature introduces support for handheld (PocketPC and Palm) based Movian VPN clients, securely extending access to your network to mobile employees and business partners.</p> <p>New support for Diffie-Hellman Group 7 (ECC) to negotiate perfect forward secrecy was added to Version 7.0. This option is intended for use with the MovianVPN client, but can be used with other clients that support D-H Group 7 (ECC).</p>
VPN NAT Transparency	<p>This feature extends support for site-to-site and remote-access IPSec-based VPNs to network environments that implement NAT or PAT, such as airports, hotels, wireless hot spots, and broadband environments. Version 7.0 also adds support for Cisco TCP and User Datagram Protocol (UDP) NAT traversal methods as complementary methods to existing support for the IETF UDP wrapper mechanism for safe traversal through NAT/PAT boundaries.</p> <p>See the <b>isakmp</b> global configuration command for additional options when configuring a NAT traversal policy.</p>
IKE Syslog Support	This feature introduces a small enhancement to IKE syslogging support and a limited set of IKE event tracing capabilities for scalable VPN troubleshooting. These enhancements have been added to allow for new syslog message generation and improved ISAKMP command control.
Diffie-Hellman (DH) Group 5 Support	This release supports the 1536-bit MODP Group that has been given the group 5 identifier.
Advanced Encryption Standard (AES)	This feature adds support for securing site-to-site and remote access VPN connections with the new international encryption standard. It also provides software-based AES support on all supported the ASA models and hardware-accelerated AES via the new VAC+ card.
New Ability to Assign Netmasks with Address Pools	This feature introduces the ability to define a subnet mask for each address pool and pass this information onto the client.
Cryptographic Engine Known Answer Test (KAT)	The function of KAT is to test the instantiation of the ASA crypto engine. The test will be performed every time during the ASA boot up before the configuration is read from Flash memory. KAT will be run for valid crypto algorithms for the current license on the ASA.
Custom Backup Concentrator Timeout	<p>This feature constitutes a configurable time out on the ASA connection attempts to a VPN headend, thereby controlling the latency involved in rolling over to the next backup concentrator on the list.</p> <p>This feature supports the <b>vpngroup</b> command.</p>
<b>WebVPN Features</b>	

**Table 49**      ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Remote Access via Web Browser (WebVPN)	Version 7.0(1) supports WebVPN on ASA 5500 series security appliances in single, routed mode. WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.
CIFS	WebVPN supports the Common Internet Files System, which lets remote users browse and access preconfigured NT/Active Directory file servers and shares at a central site. CIFS runs over TCP/IP and uses DNS and NetBIOS for name resolution.
Port Forwarding	WebVPN port forwarding, also called application access, lets remote users use TCP-applications over an SSL VPN connection.
Email	<p>WebVPN supports several ways of using email, including IMAP4S, POP3S, SMTPS, MAPI, and Web Email.</p> <ul style="list-style-type: none"> <li>• IMAP4S, POP3S, SMTPS WebVPN lets remote users use the IMAP4, POP3, and SMTP email protocols over SSL connections.</li> <li>• MAPI Proxy WebVPN supports MAPI, which is remote access to e-mail via MS Outlook Exchange port forwarding. MS Outlook exchange must be installed on the remote computer.</li> <li>• Web Email Web email is MS Outlook Web Access for Exchange 2000, Exchange 5.5, and Exchange 2003. It requires an MS Outlook Exchange Server at the central site.</li> </ul>
<b>Routing Features</b>	
IPv6 Inspection, Access Control, and Management	This feature introduces support for IP version 6 (IPv6) inspection, access control, and management. Full stateful inspection is provided for through-the-box IPv6 traffic in both a dedicated IPv6 mode and in a dual-stack IPv4 / IPv6 mode. In addition, a ASA can be deployed in a pure IPv6 environment, supporting IPv6 to-the-box management traffic for protocols including SSHv2, Telnet, HTTP, and ICMP. Inspection engines that support IPv6 traffic in Version 7.0 include HTTP, FTP, SMTP, UDP, TCP and ICMP.
DHCP Option 66 and 150 Support	<p>This feature enhances the DHCP server on the inside interface of the ASA to provide TFTP address information to the served DHCP clients. The implementation responds with one TFTP server for DHCP option 66 requests and with, at most, two servers for DHCP option 150 requests.</p> <p>DHCP options 66 and 150 simplify remote deployments of Cisco IP Phones and Cisco SoftPhone by providing the Cisco CallManager contact information needed to download the rest of the IP phone configuration.</p>

**Table 49**      **New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)**

Feature	Description
DHCP Server Support on Multiple Interfaces	<p>This release allows as many integrated Dynamic Host Configuration Protocol (DHCP) servers to be configured as desired, and on any interface. DHCP client can be configured only on the outside interface, and DHCP relay agent can be configured on any interface. However, DHCP server and DHCP relay agent cannot be configured concurrently on the same ASA, but DHCP client and DHCP relay agent can be configured concurrently.</p> <p>We modified the following command: <b>dhcpd address</b>.</p>
Multicast Support	<p>PIM sparse mode was added to allow direct participation in the creation of a multicast tree using PIM-SM. This capability extends existing multicast support for IGMP forwarding and for Class D access control policies and ACLs. PIM-SM provides an alternative to transparent mode operation in multicast environments.</p> <p>The <b>pim</b> commands and the <b>multicast-routing</b> command added support to the new functionality in addition to the <b>show mrib EXEC</b> command in this feature.</p>
<b>Interface Features</b>	
Common Security-Level for Multiple Interfaces	<p>This feature extends the security-level policy structure by enabling multiple interfaces to share a common security level. This allows for simplified policy deployments by allowing interfaces with a common security policy (for example two ports connected into the same DMZ, or multiple zones/departments within a network) to share a common security level. Communication between interfaces with the same security level is governed by the ACL on each interface.</p> <p>See the <b>same-security-traffic</b> command and the <b>inter-interface</b> keyword to enable traffic between interfaces configured with the same security level.</p>
<b>show interface</b> Command	The <b>show interface</b> command has display buffer counters.
Dedicated Out-of-Band Management Interface	The <b>management-only</b> configuration command has been introduced in the interface configuration mode to enable dedicated out-of-band management access to the device.
Modification to GE Hardware Speed Settings	The Gigabit Ethernet cards can be configured by hardware in TBI or GMII mode. TBI mode does not support half duplex. GMII mode supports both half duplex and full duplex. All the i8255x controllers used in the ASAs are configured for TBI and thus cannot support half-duplex mode, hence the half-duplex setting is removed.
VLAN-based virtual interfaces	<p>802.1Q VLAN support provides flexibility in managing and provisioning the ASA. This feature enables the decoupling of IP interfaces from physical interfaces (hence making it possible to configure logical IP interfaces independent of the number of interface cards installed), and supplies appropriate handling for IEEE 802.1Q tags.</p> <p>We introduced the following command: <b>vlan</b>.</p>
<b>NAT Features</b>	
Optional Address Translation Services	<p>This feature simplifies deployment of the ASA by eliminating previous requirement for address translation policies to be in place before allowing network traffic to flow. Now, only hosts and networks that require address translation will need to have address translation policies configured. This feature introduces a new configuration option, “nat-control”, which allows NAT to be enabled incrementally.</p> <p>Version 7.0 introduces the <b>nat-control</b> command and preserves the current behavior for customers upgrading from previous versions of the software. For new security appliances or devices which have their configurations cleared, the default will be to not require a NAT policy for traffic to traverse the security appliance.</p>
<b>High Availability Features</b>	

**Table 49**      **New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)**

Feature	Description
Active/Active Failover with Asymmetric Routing Support	<p>This feature builds upon the award-winning ASA high availability architecture, introducing support for Active/Active failover. This enables two UR licensed or one UR and one FO-AA licensed ASA to act as a failover pair, both actively passing traffic at the same time, and with Asymmetric Routing Support. The Active/Active failover feature leverages the security context feature of this software release – where each ASA in a failover pair is active for one context and standby for the other, as an inverse symmetric pair. Another key customer challenge that we are addressing in Version 7.0 is Asymmetric Routing Support. This will enable customers with advanced routing topologies, where packets may enter from one ISP and exit via another ISP, to deploy the ASA to protect those environments (leveraging the Asymmetric Routing Support introduced in Version 7.0).</p> <p>To support the Active/Active feature, the <b>failover active</b> command is extended with the <b>group</b> keyword and this software release introduces the failover group configuration mode. In addition, the <b>asr-group</b> command in interface configuration mode extends the Active/Active solution to environments with Asymmetric Routing.</p>
VPN Stateful Failover	<p>This feature introduces Stateful Failover for VPN connections, complementing the award-winning firewall failover services. All security association (SA) state information and key material is automatically synchronized between the failover pair members, providing a highly resilient VPN solution.</p> <p>The VPN Stateful Failover is enabled implicitly when the device operates in single routed mode. In addition to the <b>show failover EXEC</b> command, which includes a detailed view of VPN Stateful Failover operations and statistics, the <b>show isakmp sa</b>, <b>show ipsec sa</b> and <b>show vpnd-sessiondb</b> commands have information about the tunnels on both the active and standby unit.</p>
Failover Enhancements	This feature enhances failover functionality so that the standby unit in a ASA failover pair can be configured to use a virtual MAC address. This eliminates potential “stale” ARP entry issues for devices connected to the ASA failover pair, in the unlikely event that both ASAs in a failover pair fail at the same time and only the standby unit remains operational.
<b>show failover</b> Command	This new feature enhances the <b>show failover</b> command to display the last occurrence of a failover.
Failover Support for HTTP	<p>This feature supports the <b>failover replicate http</b> and <b>show failover</b> commands to allow the stateful replication of HTTP sessions in a Stateful Failover environment:</p> <p>When HTTP replication is enabled, the <b>show failover</b> command displays the <b>failover replicate http</b> command.</p>
Zero-Downtime Software Upgrades	This feature introduces the ability for customers to perform software upgrades of failover pairs without impacting network uptime or connections flowing through the units. Version 7.0 introduces the ability to do inter-version state sharing between ASA failover pairs, allowing customers to perform software upgrades to maintenance releases (for example Version 7.0(1) upgrading to 7.0(2)) without impacting traffic flowing through the pair (in active/standby failover environments or Active/Active environments where the pair is not oversubscribed – more that 50% load on each pair member).
General High Availability Enhancements	<p>This feature includes many significant enhancements to the Failover operation and configuration to deliver faster Failover transitions, increased scalability and even further robustness in failover operation.</p> <p>The release introduces the following new commands: <b>failover interface-policy</b>, <b>failover polltime</b>, and <b>failover reload-standby</b>.</p>

**Table 49**      **New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)**

Feature	Description
<b>Troubleshooting and Monitoring Features</b>	
Improved SNMP Support	This feature adds support for SNMPv2c, providing new services including 64-bit counters (useful for packet counters on Gigabit Ethernet interfaces) and support for bulk MIB data transfers. Additionally, Version 7.0 includes SNMPv2 MIB (RFC 1907), and the IF-MIB (RFCs 1573 and 2233) and the Cisco IPSec Flow Monitoring MIB, giving complete visibility into VPN flow statistics including tunnel uptime, bytes/packets transferred, and more.
CPU Utilization Monitoring Through SNMP	This feature supports monitoring of the ASA CPU usage through SNMP. CPU usage information is still available directly on the ASA through the <b>show cpu [usage]</b> command, but SNMP provides integration with other network management software.
SNMP Enhancements	Support for the ASA platform-specific object IDs has been added to the <b>SNMP mib-2.system.sysObjectID</b> variable. This enables CiscoView Support on the ASA.
Stack Trace in Flash Memory	This feature enables the stack trace to be stored in non-volatile Flash Memory, so that it can be retrieved at a later time for debug/troubleshooting purposes.
ICMP Ping Services	<p>This feature introduces several additions to ping (ICMP echo) services, including support for IPv6 addresses. The <b>ping</b> command also supports extended options including data pattern, df-bit, repeat count, datagram size, interval, verbose output, and sweep range of sizes.</p> <p>The existing <b>ping EXEC</b> command has been extended with various keywords and parameters to aid in troubleshooting network connectivity issues. It also provides support for an interactive mode of operation.</p>
System Health Monitoring and Diagnostic Services	This feature provides improved monitoring of the system operation and to help isolate potential network and ASA issues. The <b>show resource</b> and <b>show counters</b> commands provide detailed information about resource utilization for the appliance and security contexts as well as detailed statistics. To monitor the CPU utilization you may use the new <b>show cpu EXEC</b> command as well as the <b>show process cpu-hog EXEC</b> commands. To isolate potential software flaws the software introduces the <b>checkheaps</b> command and related <b>show EXEC</b> command. Finally, to get a better understanding of the block (packet) utilization, the <b>show blocks EXEC</b> command provides extensive analytical tools on block queuing and utilization in the system.
Debug Services	The <b>debug</b> commands have been improved and many new features include to respective debug support. Furthermore, the debug output is now supported to all virtual terminals without restrictions. That is, when you enable debug output for a particular feature, you will be able to view the output without any limitations. Clearly, the output will be restricted to the session where it was enabled. Finally, the user can send debug output over syslogs if your security policy allows it and you wish to do so by leveraging the <b>logging</b> command.
SSL debug Support	Support for the Secure Sockets Layer (SSL) protocol is added to the <b>debug</b> command. SSL is a protocol for authenticated and encrypted communications between client and servers such as the ASDM and the ASA.

**Table 49**      ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)***

Feature	Description
Packet Capture	<p>This release supports packet capture. The ASA packet capture provides the ability to sniff or “see” any traffic accepted or blocked by the ASA. Once the packet information is captured, you have the option of viewing it on the console, transferring it to a file over the network using a TFTP server, or accessing it through a web browser using Secure HTTP. However, the ASA does not capture traffic unrelated to itself on the same network segment, and this packet capture feature does not include file system, DNS name resolution, or promiscuous mode support.</p> <p>Users can now specify the <b>capture</b> command to store the packet capture in a circular buffer. The capture will continue writing packets to the buffer until it is stopped by the administrator.</p> <p>The ASA introduces additional support to improve the ability of the user to diagnose device operation by supporting the ability to capture ISAKMP traffic and only capture packets dropped by the new Accelerated Security Path (ASP).</p> <p>The existing <b>capture</b> command has been extended with a new <b>type</b> keyword and parameters to capture ISAKMP, packet drops, and packet drops matching a specified reason string.</p>
<b>show tech</b> Command	This feature enhances the current <b>show tech</b> command output to include additional diagnostic information.
<b>Management Features</b>	
Storage of Multiple Configurations in Flash Memory	<p>This release debuts a new Flash file system on the ASA enabling administrators to store multiple configurations on the security appliance. This provides the ability to do configuration roll-back in the event of a mis-configuration. Commands are introduced to manage files on this new file system.</p> <p><b>Note</b>    The new Flash file system is capable of storing not only configuration files but also multiple system images and multiple PIX images when there is adequate Flash space available.</p> <p>The <b>boot config</b> global configuration command provides the ability to specify which configuration file should be used at start-up.</p>
Secure Asset Recovery	This feature introduces the ability to prevent the recovery of configuration data, certificates and key material if the <b>no service password recovery</b> command is in an ASA's configuration (while still allowing customers to recover the asset). This feature is useful in environments where physical security may not be ideal, and to prevent nefarious individuals gaining access to sensitive configuration data.
Scheduled System Reload (Reboot)	Administrators now have the ability to schedule a reload on an ASA either at a specific time, or at an offset from the current time, thus making it simpler to schedule network downtimes and notify remote access VPN users of an impending reboot.
Command-Line Interface (CLI) Usability	This feature enhances the CLI “user experience” by incorporating many popular Cisco IOS software command-line services such as command completion, online help, and aliasing for improved ease-of-use and common user experience.
Command-Line Interface (CLI) Activation Key Management	This feature lets you enter a new activation key through the ASA command-line interface (CLI), without using the system monitor mode and having to TFTP a new image. Additionally, the ASA CLI displays the currently running activation key when you enter the <b>show version</b> command.
<b>show version</b> Command	The <b>show version</b> command output now has two interface-related lines, Max Physical interfaces and Max interfaces. Max interfaces is the total physical and virtual interfaces.
<b>AAA Features</b>	

**Table 49**      ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
AAA Integration	Version 7.0(1) native integration with authentication services including Kerberos, NT Domain, and RSA SecurID (without requiring a separate RADIUS/TACACS+ server) for simplified VPN user authentication. This release also introduces the ability to generate TACACS+AAA accounting records for tracking administrative access to ASAs, as well as tracking all configuration changes that are made during an administrative session.
AAA Fallback for Administrative Access	This feature introduces the ability to authenticate and authorize requests to fall-back to a local user database on the ASA. The requirements and design will factor future compatibility with Cisco IOS software-like “method list” support for the ASA, and deliver the addition of the LOCAL fallback method.
AAA Integration Enhancements	This feature debuts native integration with authentication services including Kerberos, LDAP, and RSA SecurID (without requiring a separate RADIUS/TACACS+ server) for simplified user and administrator authentication. This feature also introduces the ability to generate TACACS+AAA accounting records for tracking administrative access to ASAs, as well as tracking all configuration changes that are made during an administrative session.
Secure HyperText Transfer Protocol (HTTPS) Authentication Proxy	<p>This feature extends the capabilities of the ASA to securely authenticate HTTP sessions and adds support for HTTPS Authentication Proxy. To configure secure authentication of HTTP sessions, use the <b>aaa authentication secure-http-client</b> command. To configure secure authentication of HTTPS sessions, use the <b>aaa authentication include https</b> or the <b>aaa authentication include tcp/0</b> command.</p> <p>In this release configurations that include the <b>aaa authentication include tcp/0</b> command will inherit the HTTPS Authentication Proxy feature, which is enabled by default with a code upgrade to Version 6.3 or later.</p>
Downloadable Access Control Lists (ACLs)	<p>This feature supports the download of ACLs to the ASA from an access control server (ACS). This enables the configuration of per-user access lists on a AAA server, to provide per-user access list authorization, that are then downloadable through the ACS to the ASA.</p> <p>This feature is supported for RADIUS servers only and is not supported for TACACS+ servers.</p>
New Syslog Messaging for AAA authentication	This feature introduces a new AAA syslog message, which prompts users for their Authentication before they can use a service port.
Per-user-override	This feature allows users to specify a new keyword per-user-override to the <b>access-group</b> command. When this keyword is specified, it allows the permit/deny status from the per-user access-list (downloaded via AAA authentication) that is associated to a user to override the permit/deny status from the access-group access-list.
Local User Authentication Database for Network and VPN Access	<p>This feature allows cut-through and VPN (using xauth) traffic to be authenticated using the ASA local username database (as an alternative in addition to the existing authenticating via an external AAA server).</p> <p>The server tag variable now accepts the value LOCAL to support cut-through proxy authentication using Local Database.</p>
<b>ASDM Features</b>	
Dynamic Dashboard (ASDM Home Page)	<ul style="list-style-type: none"> <li>Displays detailed device and licensing information for quick identification of system and resources available.</li> <li>Displays real-time system and traffic profiling .</li> </ul>
Real-time Log Viewer	<ul style="list-style-type: none"> <li>Displays real-time syslog messages.</li> <li>Advanced filtering capabilities make it easy to focus on key events.</li> </ul>

**Table 49**      ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)***

<b>Feature</b>	<b>Description</b>
Improved Java Web-Based Architecture	<ul style="list-style-type: none"> <li>• Accelerates the loading of ASDM with optimized applet caching capability.</li> <li>• Provides anytime, anywhere access to all management and monitoring features.</li> </ul>
Downloadable ASDM Launcher (on Microsoft Windows 2000 or XP operating systems only)	<ul style="list-style-type: none"> <li>• Lets you download and run ASDM locally on your PC.</li> <li>• Multiple instances of ASDM Launcher provide administrative access to multiple security appliances simultaneously, from the same management workstation.</li> <li>• Automatically updates the software based on the installed version on the appliance, enabling consistent security management throughout the network.</li> </ul>
Multiple Language Operating System Support	Supports both the English and Japanese versions of the Microsoft Windows operating systems.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2011-2013 Cisco Systems, Inc. All rights reserved.





