Introduction to the Cisco ASA

The Cisco ASA provides advanced stateful firewall and VPN concentrator functionality in one device, and for some models, integrated services modules such as IPS. The ASA includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), clustering (combining multiple firewalls into a single firewall), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPsec VPN, SSL VPN, and clientless SSL VPN support, and many more features.

Note ASDM supports many ASA versions. The ASDM documentation and online help includes all of the latest features supported by the ASA. If you are running an older version of ASA software, the documentation might include features that are not supported in your version. Similarly, if a feature was added into a maintenance release for an older major or minor version, then the ASDM documentation includes the new feature even though that feature might not be available in all later ASA releases. Please refer to the feature history table for each chapter to determine when features were added. For the minimum supported version of ASDM for each ASA version, see *Cisco ASA 5500 Series Hardware and Software Compatibility*.

This chapter includes the following sections:

ASDM Client Operating System and Browser Requirements

Table 1-1 lists the supported and recommended client operating systems and Java for ASDM.

Table 1-1 Operating System and Browser Requirements

Operating System	Browser				Java SE Plug-in
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): • 7 • Vista • 2008 Server • XP	6.0 or later	1.5 or later	No support	18.0 or later	6.0 or later
Apple Macintosh OS X: • 10.8 • 10.7 • 10.6 • 10.5 • 10.4	No support	1.5 or later	2.0 or later	18.0 or later	6.0 or later
Red Hat Enterprise Linux 5 (GNOME or KDE): • Desktop • Desktop with Workstation	N/A	1.5 or later	N/A	18.0 or later	6.0 or later

See the following caveats:

- If you upgrade from a previous version to Java 7 update 5, you may not be able to open ASDM using the Java Web Start from an IPv6 address; you can either download the ASDM Launcher, or follow the instructions at: http://java.com/en/download/help/clearcache_upgrade.xml.
- ASDM requires you to make an SSL connection to the ASA in the following situations:
  - When you first connect your browser to the ASA and access the ASDM splash screen.
  - When you launch ASDM using the launcher or the Java web start application.

  If the ASA only has the base encryption license (DES), and therefore has weak encryption ciphers for the SSL connection, you may not be able to access the splash screen or launch ASDM. See the following issues:
  - When using Java 7 when launching ASDM, you must have the strong encryption license (3DES/AES) on the ASA. With only the base encryption license (DES), you cannot launch ASDM. Even if you can connect with a browser to the ASDM splash screen and download the launcher or web start application, you cannot then launch ASDM. You must uninstall Java 7, and install Java 6.
  - When using Java 6 for accessing the splash screen in a browser, by default, Internet Explorer on Windows Vista and later and Firefox on all operating systems do not support DES for SSL; therefore without the strong encryption license (3DES/AES), see the following workarounds:

If available, use an already downloaded ASDM launcher or Java web start application. The launcher works with Java 6 and weak encryption, even if the browsers do not.

For Windows Internet Explorer, you can enable DES as a workaround. See http://support.microsoft.com/kb/929708 for details.

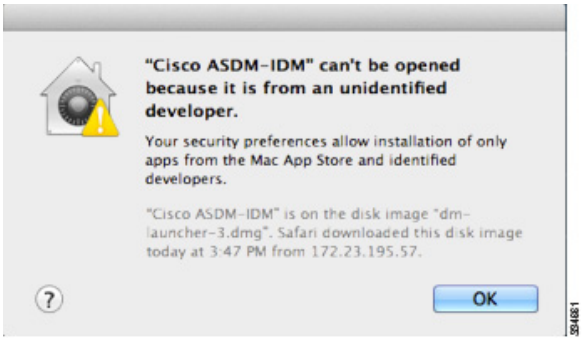
For Firefox on any operating system, you can enable the security.ssl3.dhe_dss_des_sha setting as a workaround. See http://kb.mozillazine.org/About:config to learn how to change hidden configuration preferences.

- When the ASA uses a self-signed certificate or an untrusted certificate, Firefox 4 and later and Safari are unable to add security exceptions when browsing using HTTPS over IPv6. See: https://bugzilla.mozilla.org/show_bug.cgi?id=633001. This caveat affects all SSL connections originating from Firefox or Safari to the ASA (including ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority.
- If you change the SSL encryption on the ASA to exclude both RC4-MD5 and RC4-SHA1 algorithms (these algorithms are enabled by default), then Chrome cannot launch ASDM due to the Chrome "SSL false start" feature. We suggest re-enabling one of these algorithms (see the Configuration > Device Management > Advanced > SSL Settings pane); or you can disable SSL false start in Chrome using the **--disable-ssl-false-start** flag according to http://www.chromium.org/developers/how-tos/run-chromium-with-flags.
- For Internet Explorer 9.0 for servers, the "Do not save encrypted pages to disk" option is enabled by default (See Tools > Internet Options > Advanced). This option causes the initial ASDM download to fail. Be sure to disable this option to allow ASDM to download.
- On MacOS, you may be prompted to install Java the first time you run ASDM; follow the prompts as necessary. ASDM will launch after the installation completes.
- On MacOS, you may see the following error message when opening the ASDM Launcher:

```
Cannot launch Cisco ASDM-IDM. No compatible version of Java 1.5+ is available.
```

In this case, Java 7 is the currently-preferred Java version; you need to set Java 6 as the preferred Java version: Open the **Java Preferences** application (under Applications > Utilities), select the preferred Java version, and drag it up to be the first line in the table.

- On MacOS 10.8 and later, you need to allow applications that are not signed with an Apple Developer ID. If you do not change your security preferences, you see an error screen.



a. To change the security setting, open System Preferences, and click **Security & Privacy**.

b. On the General tab, under Allow applications downloaded from, click **Anywhere**.

Hardware and Software Compatibility

For a complete list of supported hardware and software, see the *Cisco ASA Compatibility*:
http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN Specifications

See *Supported VPN Platforms, Cisco ASA 5500 Series*:
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

New Features

Note New, changed, and deprecated syslog messages are listed in syslog messages guide.

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

Released: July 22, 2013

Table 1-3 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 1-2 New Features for ASA Version 9.0(3)/ASDM Version 7.1(3)

Feature	Description
Monitoring Features	
Smart Call Home	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: • When a unit joins the cluster • When a unit leaves the cluster • When a cluster unit becomes the cluster master Each message that is sent includes the following information: • The active cluster member count • The output of the **show cluster info** command and the **show cluster history** command on the cluster master

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

Released: February 25, 2013

Table 1-3 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 1-3 New Features for ASA Version 9.0(2)/ASDM Version 7.1(2)

Feature	Description
Remote Access Features	
Clientless SSL VPN: Windows 8 Support	This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems. We support the following browsers on Windows 8: • Internet Explorer 10 (desktop only) • Firefox (all supported Windows 8 versions) • Chrome (all supported Windows 8 versions) See the following limitations: • Internet Explorer 10: – The Modern (AKA Metro) browser is not supported. – If you enable Enhanced Protected Mode, we recommend that you add the ASA to the trusted zone. – If you enable Enhanced Protected Mode, Smart Tunnel and Port Forwarder are not supported. • A Java Remote Desktop Protocol (RDP) plugin connection to a Windows 8 PC is not supported.
Cisco Secure Desktop: Windows 8 Support	CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check. See the following limitations: • Secure Desktop (Vault) is not supported with Windows 8.
Dynamic Access Policies: Windows 8 Support	ASDM was updated to enable selection of Windows 8 in the DAP Operating System attribute.
Management Features	
The default Telnet password was removed	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. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication. Formerly, when you cleared the password, the ASA restored the default of "cisco." Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASASM (see the **session** command). For initial ASASM access, you must use the **service-module session** command, until you set a login password. We did not modify any ASDM screens.

Released: October 31, 2012

Table 1-4 lists the new features for ASA Version 8.4(5).

Table 1-4 New Features for ASA Version 8.4(5)

Feature	Description
Firewall Features	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL. We modified the following command: **access-list ethertype** {**permit** | **deny**} **is-is**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
ARP cache additions for non-connected subnets	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. You may want to use this feature if you use: • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. We introduced the following command: **arp permit-nonconnected**. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Increased maximum connection limits for service policy rules	The maximum number of connections for service policy rules was increased from 65535 to 2000000. We modified the following commands: **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, **set connection per-client-max**. *This feature is not available in 8.5(1), 8.6(1), or 8.7(1).*
Remote Access Features	
Improved Host Scan and ASA Interoperability	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. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
Monitoring Features	
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 **show xlate count** command. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*
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 the following command: **flow-export active refresh-interval**. We modified the following command: **flow-export event-type**. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*

Table 1-4 New Features for ASA Version 8.4(5) (continued)

Feature	Description
Hardware Features	
ASA 5585-X DC power supply support	Support was added for the ASA 5585-X DC power supply. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).*

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

Released: October 29, 2012

Table 1-5 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 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1)

Feature	Description
Firewall Features	
Cisco TrustSec integration	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. 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. 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. We introduced the following MIB: CISCO-TRUSTSEC-SXP-MIB. We introduced or modified the following screens: Configuration > Firewall > Identity by TrustSec Configuration > Firewall > Objects > Security Groups Object Groups Configuration > Firewall > Access Rules > Add Access Rules Monitoring > Properties > Identity by TrustSec > PAC Monitoring > Properties > Identity by TrustSec > Environment Data Monitoring > Properties > Identity by TrustSec > SXP Connections Monitoring > Properties > Identity by TrustSec > IP Mappings Monitoring > Properties > Connections Tools > Packet Tracer

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Cisco Cloud Web Security (ScanSafe)	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. **Note** 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. We introduced or modified the following screens: Configuration > Device Management > Cloud Web Security Configuration > Firewall > Objects > Class Maps > Cloud Web Security Configuration > Firewall > Objects > Class Maps > Cloud Web Security > Add/Edit Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security > Add/Edit Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security > Add/Edit > Manage Cloud Web Security Class Maps Configuration > Firewall > Identity Options Configuration > Firewall > Service Policy Rules Monitoring > Properties > Cloud Web Security
Extended ACL and object enhancement to filter ICMP traffic by ICMP code	ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following screens: Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > Access Rule
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.
Per-session PAT	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*. 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. We introduced the following screen: Configuration > Firewall > Advanced > Per-Session NAT Rules.

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
ARP cache additions for non-connected subnets	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. You may want to use this feature if you use: • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. We modified the following screen: Configuration > Device Management > Advanced > ARP > ARP Static Table. *Also available in 8.4(5).*
SunRPC change from dynamic ACL to pin-hole mechanism	Previously, Sun RPC inspection does not support outbound access lists because the inspection engine uses dynamic access lists instead of secondary connections. 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. *Also available in 8.4(4.1).*
Inspection reset action change	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. 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: • The ASA sends a TCP reset to the inside host when the **service resetoutbound** command is enabled. (The **service resetoutbound** command is disabled by default.) • The ASA sends a TCP reset to the outside host when the **service resetinbound** command is enabled. (The **service resetinbound** command is disabled by default.) For more information, see the **service** command in the ASA command reference. 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. *Also available in 8.4(4.1).*

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Increased maximum connection limits for service policy rules	The maximum number of connections for service policy rules was increased from 65535 to 2000000. We modified the following screen: Configuration > Firewall > Service Policy Rules > Connection Settings. *Also available in 8.4(5)*
High Availability and Scalability Features	
ASA Clustering for the ASA 5580 and 5585-X	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. We introduced or modified the following screens: Home > Device Dashboard Home > Cluster Dashboard Home > Cluster Firewall Dashboard Configuration > Device Management > Advanced > Address Pools > MAC Address Pools Configuration > Device Management > High Availability and Scalability > ASA Cluster Configuration > Device Management > Logging > Syslog Setup > Advanced Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced Configuration > Device Setup > Interfaces > Add/Edit Interface > IPv6 Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface > Advanced Configuration > Firewall > Advanced > Per-Session NAT Rules Monitoring > ASA Cluster Monitoring > Properties > System Resources Graphs > Cluster Control Link Tools > Preferences > General Tools > System Reload Tools > Upgrade Software from Local Computer Wizards > High Availability and Scalability Wizard Wizards > Packet Capture Wizard Wizards > Startup Wizard
OSPF, EIGRP, and Multicast for clustering	For OSPFv2 and OSPFv3, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment. For EIGRP, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment. Multicast routing supports clustering.

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Packet capture for clustering	To support cluster-wide troubleshooting, you can enable capture of cluster-specific traffic on the master unit using the **cluster exec capture** command, which is then automatically enabled on all of the slave units in the cluster. The **cluster exec** keywords are the new keywords that you place in front of the **capture** command to enable cluster-wide capture. We modified the following screen: Wizards > Packet Capture Wizard.
Logging for clustering	Each unit in the cluster generates syslog messages independently. You can use the **logging device-id** 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. We modified the following screen: Configuration > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration.
Configure the connection replication rate during a bulk sync	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. *Also available in 8.4(4.1) and 8.5(1.7).*
IPv6 Features	
IPv6 Support on the ASA's outside interface for VPN Features.	This release of the ASA adds support for IPv6 VPN connections to its outside interface using SSL and IKEv2/IPsec protocols. 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.
Remote Access VPN support for IPv6: IPv6 Address Assignment Policy	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. The endpoint must have the dual-stack protocol implemented in its operating system to be assigned both types of addresses. Assigning an IPv6 address to the client is supported for the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol. We modified the following screens: Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy Configuration > Remote Access VPN > AAA/Local Users > Local Users > (Edit local user account) > VPN Policy

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Remote Access VPN support for IPv6: Assigning DNS Servers with IPv6 Addresses to group policies	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. 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. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Servers.
Remote Access VPN support for IPv6: Split tunneling	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. 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. 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. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Advanced > Split Tunneling.
Remote Access VPN support for IPv6: AnyConnect Client Firewall Rules	Access control rules for client firewalls support access list entries for both IPv4 and IPv6 addresses. 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. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Advanced > AnyConnect Client > Client Firewall.

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Remote Access VPN support for IPv6: Client Protocol Bypass	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. 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." 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. This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Group Policy) Advanced > AnyConnect Client > Client Bypass Protocol.
Remote Access VPN support for IPv6: IPv6 Interface ID and prefix	You can now specify a dedicated IPv6 address for local VPN users. This feature benefits users configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol. We modified the following screen: Configuration > Remote Access VPN > AAA/Local Users > Local Users > (Edit User) > VPN Policy.
Remote Access VPN support for IPv6: Sending ASA FQDN to AnyConnect client	You can return the FQDN of the ASA to the AnyConnect client to facilitate load balancing and session roaming. This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol. We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Advanced > AnyConnect.
Remote Access VPN support for IPv6: ASA VPN Load Balancing	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. 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. This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol. We modified the following screen: Configuration > Remote Access VPN > Load Balancing.

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Remote Access VPN support for IPv6: Dynamic Access Policies support IPv6 attributes	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): • IPv6 addresses as a Cisco AAA attribute • IPv6 TCP and UDP ports as part of a Device endpoint attribute • Network ACL Filters (client) This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol. We modified the following screens: Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add > Cisco AAA attribute Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add > Device > Add Endpoint Attribute Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Network ACL Filters (client) Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Webtype ACL Filters (clientless)
Remote Access VPN support for IPv6: Session Management	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. This feature can be used by clients configured to use the SSL protocol. This feature does not support IKEv2/IPsec protocol. We modified these screen: Monitoring > VPN > VPN Statistics > Sessions.
NAT support for IPv6	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. We modified the following screens: Configuration > Firewall > Objects > Network Objects/Group Configuration > Firewall > NAT Rules
DHCPv6 relay	DHCP relay is supported for IPv6. We modified the following screen: Configuration > Device Management > DHCP > DHCP Relay.

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
OSPFv3	OSPFv3 routing is supported for IPv6. Note the following additional guidelines and limitations for OSPFv2 and OSPFv3: **Clustering** • OSPFv2 and OSPFv3 support clustering. • When clustering is configured, OSPFv3 encryption is not supported. An error message appears if you try to configure OSPFv3 encryption in a clustering environment. • When using individual interfaces, make sure that you establish the master and slave units as either OSPFv2 or OSPFv3 neighbors. • 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. **Other** • OSPFv2 and OSPFv3 support multiple instances on an interface. • The ESP and AH protocol is supported for OSPFv3 authentication. • OSPFv3 supports Non-Payload Encryption. We introduced the following screens: Configuration > Device Setup > Routing > OSPFv3 > Setup Configuration > Device Setup > Routing > OSPFv3 > Interface Configuration > Device Setup > Routing > OSPFv3 > Redistribution Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix Configuration > Device Setup > Routing > OSPFv3 > Virtual Link Monitoring > Routing > OSPFv3 LSAs Monitoring > Routing > OSPFv3 Neighbors
Unified ACL for IPv4 and IPv6	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. 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. We modified the following screens: Configuration > Firewall > Access Rules Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Mixed IPv4 and IPv6 object groups	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. **Note** You cannot use a mixed object group for NAT. We modified the following screen: Configuration > Firewall > Objects > Network Objects/Groups.
Range of IPv6 addresses for a Network object	You can now configure a range of IPv6 addresses for a network object. We modified the following screen: Configuration > Firewall > Objects > Network Objects/Groups.
Inspection support for IPv6 and NAT64	We now support DNS inspection for IPv6 traffic. We also support translating between IPv4 and IPv6 for the following inspections: • DNS • FTP • HTTP • ICMP You can now also configure the service policy to generate a syslog message (767001) when unsupported inspections receive and drop IPv6 traffic. We modified the following screen: Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard - Service Policy.
Remote Access Features	
Clientless SSL VPN: Additional Support	We have added additional support for these browsers, operating systems, web technologies and applications: **Internet browser support**: Microsoft Internet Explorer 9, Firefox 4, 5, 6, 7, and 8 **Operating system support**: Mac OS X 10.7 **Web technology support**: HTML 5 **Application Support**: Sharepoint 2010
Clientless SSL VPN: Enhanced quality for rewriter engines	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. We did not add or modify any ASDM screens for this feature. *Also available in 8.4(4.1).*

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Clientless SSL VPN: Citrix Mobile Receiver	This feature provides secure remote access for Citrix Receiver applications running on mobile devices to XenApp and XenDesktop VDI servers through the ASA. 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. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policy > Edit > More Options > VDI Access > Add VDI Server.
Clientless SSL VPN: Enhanced Auto-sign-on	This feature improves support for web applications that require dynamic parameters for authentication. We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks.
Clientless SSL VPN: Clientless Java Rewriter Proxy Support	This feature provides proxy support for clientless Java plug-ins when a proxy is configured in client machines' browsers. We did not add or modify any ASDM screens for this feature.
Clientless SSL VPN: Remote File Explorer	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. We did not add or modify any ASDM screens for this feature.
Clientless SSL VPN: Server Certificate Validation	This feature enhances clientless SSL VPN support to enable SSL server certificate verification for remote HTTPS sites against a list of trusted CA certificates. We modified the following screen: Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool.
AnyConnect Performance Improvements	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. We modified the following screen: Configuration > Remote Access VPN > Advanced > Crypto Engine.
Custom Attributes	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. For AnyConnect 3.1, custom attributes are available to support AnyConnect Deferred Upgrade. Custom attributes can benefit AnyConnect clients configured for either IKEv2/IPsec or SSL protocols. A new screen was added: Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Next Generation Encryption	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. The following functionality is added to ASA to support the Suite B algorithms: • AES-GCM/GMAC support (128-, 192-, and 256-bit keys) – IKEv2 payload encryption and authentication – ESP packet encryption and authentication – Hardware supported only on multi-core platforms • SHA-2 support (256-, 384-, and 512-bit hashes) – ESP packet authentication – Hardware and software supported only on multi-core platforms • ECDH support (groups 19, 20, and 21) – IKEv2 key exchange – IKEv2 PFS – Software only supported on single- or multi-core platforms • ECDSA support (256-, 384-, and 521-bit elliptic curves) – IKEv2 user authentication – PKI certificate enrollment – PKI certificate generation and verification – Software only supported on single- or multi-core platforms New cryptographic algorithms are added for IPsecV3. **Note** 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. We introduced or modified the following screens: Monitor > VPN > Sessions Monitor > VPN > Encryption Statistics Configuration > Site-to-Site VPN > Certificate Management > Identity Certificates Configuration > Site-to-Site VPN > Advanced > System Options Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps
Support for VPN on the ASASM	The ASASM now supports all VPN features.

Table 1-5 New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)

Feature	Description
Multiple Context Mode Features	
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	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. We modified the following screen: Configuration > Context Management > Resource Class > Add Resource Class.
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	A new resource class, routes, was created to set the maximum number of routing table entries in each context. We modified the following screen: Configuration > Context Management > Resource Class > Add Resource Class.
Mixed firewall mode support in multiple context mode	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. You cannot set the firewall mode in ASDM; you must use the command-line interface. *Also available in Version 8.5(1).*
Module Features	
ASA Services Module support on the Cisco 7600 switch	The Cisco 7600 series now supports the ASASM. For specific hardware and software requirements, see: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html.
ASA 5585-X support for the ASA CX SSP-10 and -20	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. We introduced the following screens: Home > ASA CX Status Wizards > Startup Wizard > ASA CX Basic Configuration Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA CX Inspection *Also available in 8.4(4.1).*
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	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. We did not modify any screens.

How the ASA Services Module Works with the Switch

You can install the ASASM in the Catalyst 6500 series and Cisco 7600 series switches with Cisco IOS software on both the switch supervisor and the integrated MSFC.

Note The Catalyst Operating System (OS) is not supported.

The ASA runs its own operating system.

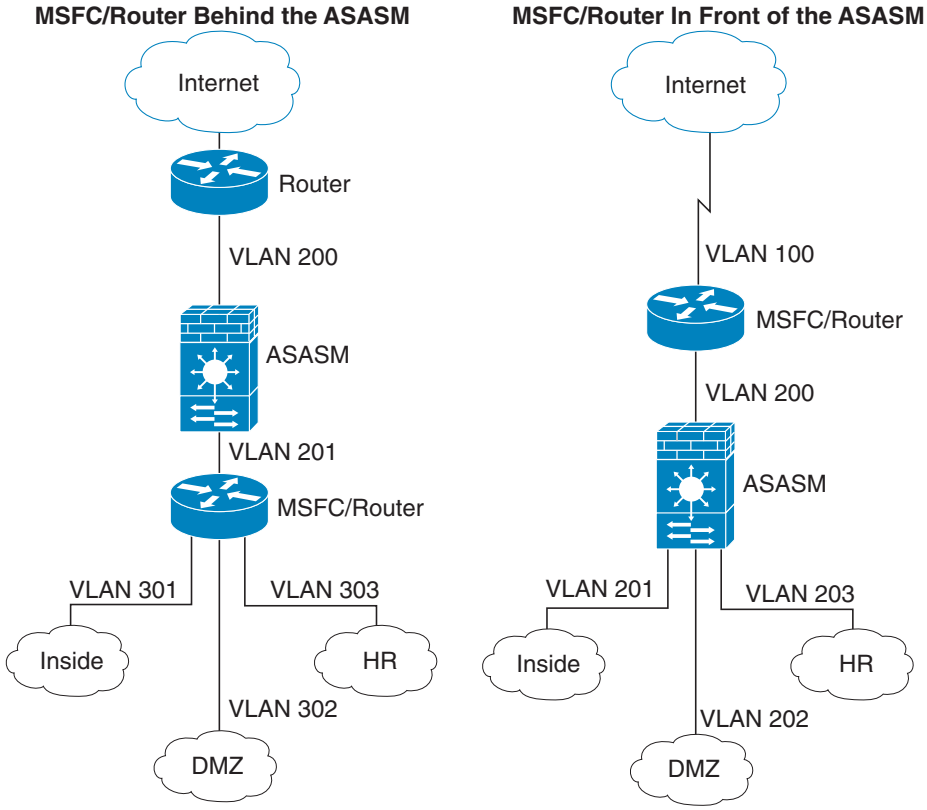
The switch includes a switching processor (the supervisor) and a router (the MSFC). Although you need the MSFC as part of your system, you do not have to use it. If you choose to do so, you can assign one or more VLAN interfaces to the MSFC. You can alternatively use external routers instead of the MSFC.

In single context mode, you can place the router in front of the firewall or behind the firewall (see Figure 1-1).

The location of the router depends entirely on the VLANs that you assign to it. For example, the router is behind the firewall in the example shown on the left side of Figure 1-1 because you assigned VLAN 201 to the inside interface of the ASASM. The router is in front of the firewall in the example shown on the right side of Figure 1-1 because you assigned VLAN 200 to the outside interface of the ASASM.

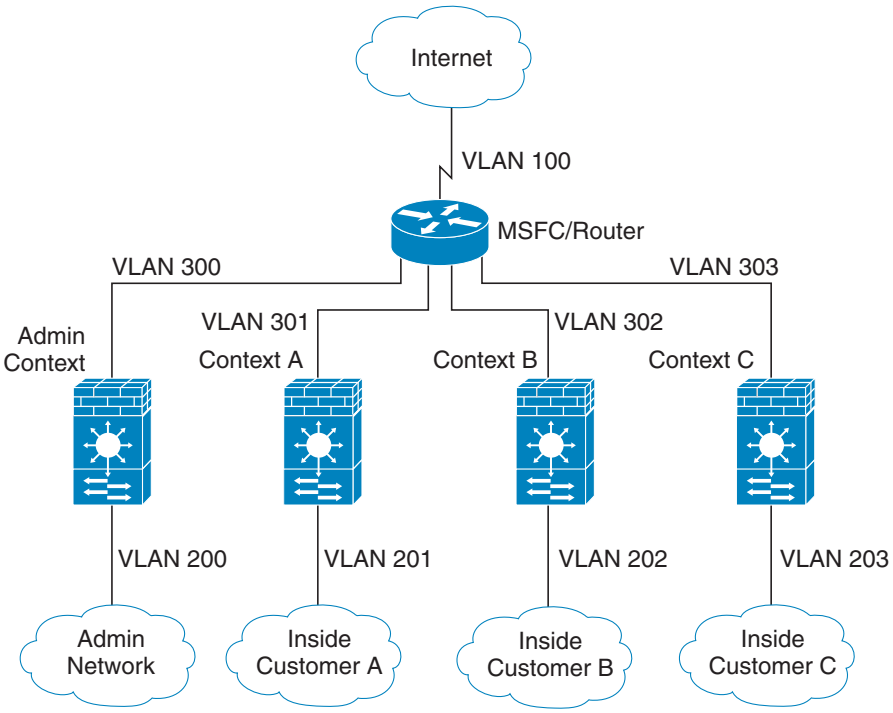
In the left-hand example, the MSFC or router routes between VLANs 201, 301, 302, and 303, and no inside traffic goes through the ASASM unless it is destined for the Internet. In the right-hand example, the ASASM processes and protects all traffic between the inside VLANs 201, 202, and 203.

Figure 1-1 MSFC/Router Placement



For multiple context mode, if you place the router behind the ASASM, you should only connect it to a single context. If you connect the router to multiple contexts, the router will route between the contexts, which might not be your intention. The typical scenario for multiple contexts is to use a router in front of all the contexts to route between the Internet and the switched networks (see Figure 1-2).

Figure 1-2 MSFC/Router Placement with Multiple Contexts



Firewall Functional Overview

Firewalls protect inside networks from unauthorized access by users on an outside network. A firewall can also protect inside networks from each other, for example, by keeping a human resources network separate from a user network. If you have network resources that need to be available to an outside user, such as a web or FTP server, you can place these resources on a separate network behind the firewall, called a *demilitarized zone* (DMZ). The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the other inside networks. You can also control when inside users access outside networks (for example, access to the Internet), by allowing only certain addresses out, by requiring authentication or authorization, or by coordinating with an external URL filtering server.

When discussing networks connected to a firewall, the *outside* network is in front of the firewall, the *inside* network is protected and behind the firewall, and a *DMZ*, while behind the firewall, allows limited access to outside users. Because the ASA lets you configure many interfaces with varied security policies, including many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

This section includes the following topics:

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the ASA allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level). You can apply actions to traffic to customize the security policy. This section includes the following topics:

Permitting or Denying Traffic with Access Rules

You can apply an access rule to limit traffic from inside to outside, or allow traffic from outside to inside. For transparent firewall mode, you can also apply an EtherType access list to allow non-IP traffic.

Applying NAT

Some of the benefits of NAT include the following:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.

Protecting from IP Fragments

The ASA provides IP fragment protection. This feature performs full reassembly of all ICMP error messages and virtual reassembly of the remaining IP fragments that are routed through the ASA. Fragments that fail the security check are dropped and logged. Virtual reassembly cannot be disabled.

Using AAA for Through Traffic

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

Applying HTTP, HTTPS, or FTP Filtering

Although you can use access lists to prevent outbound access to specific websites or FTP servers, configuring and managing web usage this way is not practical because of the size and dynamic nature of the Internet. We recommend that you use the ASA in conjunction with a separate server running one of the following Internet filtering products:

- Websense Enterprise
- Secure Computing SmartFilter

Applying Application Inspection

Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the ASA to do a deep packet inspection.

Sending Traffic to the IPS Module

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

Sending Traffic to the Content Security and Control Module

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

Applying QoS Policies

Some network traffic, such as voice and streaming video, cannot tolerate long latency times. QoS is a network feature that lets you give priority to these types of traffic. QoS refers to the capability of a network to provide better service to selected network traffic.

Applying Connection Limits and TCP Normalization

You can limit TCP and UDP connections and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. The ASA uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

TCP normalization is a feature consisting of advanced TCP connection settings designed to drop packets that do not appear normal.

Enabling Threat Detection

You can configure scanning threat detection and basic threat detection, and also how to use statistics to analyze threats.

Basic threat detection detects activity that might be related to an attack, such as a DoS attack, and automatically sends a system log message.

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the ASA scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

You can configure the ASA to send system log messages about an attacker or you can automatically shun the host.

Enabling the Botnet Traffic Filter

Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses (the blacklist), and then logs any suspicious activity. When you see syslog messages about the malware activity, you can take steps to isolate and disinfect the host.

Configuring Cisco Unified Communications

The Cisco ASA 5500 series is a strategic platform to provide proxy functions for unified communications deployments. The purpose of a proxy is to terminate and reoriginate connections between a client and server. The proxy delivers a range of security functions such as traffic inspection, protocol conformance, and policy control to ensure security for the internal network. An increasingly popular function of a proxy is to terminate encrypted connections in order to apply security policies while maintaining confidentiality of connections.

Firewall Mode Overview

The ASA runs in two different firewall modes:

- Routed

- Transparent

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

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

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

Stateful Inspection Overview

All traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process.

Note The TCP state bypass feature allows you to customize the packet flow. See the "TCP State Bypass" section on page 71-3.

A stateful firewall like the ASA, however, takes into consideration the state of a packet:

- Is this a new connection?

  If it is a new connection, the ASA has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path."

  The session management path is responsible for the following tasks:

  - Performing the access list checks
  - Performing route lookups
  - Allocating NAT translations (xlates)
  - Establishing sessions in the "fast path"

  The ASA creates forward and reverse flows in the fast path for TCP traffic; the ASA also creates connection state information for connectionless protocols like UDP, ICMP (when you enable ICMP inspection), so that they can also use the fast path.

  Note For other IP protocols, like SCTP, the ASA does not create reverse path flows. As a result, ICMP error packets that refer to these connections are dropped.

  Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that have two or more channels: a data channel, which uses well-known port numbers, and a control channel, which uses different port numbers for each session. These protocols include FTP, H.323, and SNMP.

- Is this an established connection?

If the connection is already established, the ASA does not need to re-check packets; most matching packets can go through the "fast" path in both directions. The fast path is responsible for the following tasks:

- IP checksum verification
- Session lookup
- TCP sequence number check
- NAT translations based on existing sessions
- Layer 3 and Layer 4 header adjustments

Data packets for protocols that require Layer 7 inspection can also go through the fast path.

Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection.

VPN Functional Overview

A VPN is a secure connection across a TCP/IP network (such as the Internet) that appears as a private connection. This secure connection is called a tunnel. The ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination. The ASA invokes various standard protocols to accomplish these functions.

The ASA performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

The ASA invokes various standard protocols to accomplish these functions.

Security Context Overview

You can partition a single ASA into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

In multiple context mode, the ASA includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs into the admin context, then that user has system administrator rights and can access the system and all other contexts.

ASA Clustering Overview

ASA Clustering lets you group multiple ASAs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

You perform all configuration (aside from the bootstrap configuration) on the master unit only; the configuration is then replicated to the member units.