Cisco ASA Series General Operations CLI Configuration Guide

Software Version 9.3

Released: July 24, 2014
Updated: February 18, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: N/A, Online only
About This Guide

- Document Objectives, page iii
- Related Documentation, page iii
- Conventions, page iii
- Obtaining Documentation and Submitting a Service Request, page iv

Document Objectives

The purpose of this guide is to help you configure general operations for the Cisco ASA series using the command-line interface. This guide does not cover every feature, but describes only the most common configuration scenarios.

You can also configure and monitor the ASA by using the Adaptive Security Device Manager (ASDM), a web-based GUI application. ASDM includes configuration wizards to guide you through some common configuration scenarios, and online help for less common scenarios.

Throughout this guide, the term “ASA” applies generically to supported models, unless specified otherwise.

Related Documentation

For more information, see Navigating the Cisco ASA Series Documentation at http://www.cisco.com/go/asadocs.

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
</tbody>
</table>
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
PART 1

Getting Started with the ASA
Introduction to the Cisco ASA

Released: July 24, 2014
Updated: May 7, 2015

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.

- Hardware and Software Compatibility, page 1-1
- VPN Compatibility, page 1-1
- New Features, page 1-2
- Firewall Functional Overview, page 1-10
- VPN Functional Overview, page 1-14
- Security Context Overview, page 1-14
- ASA Clustering Overview, page 1-15
- Special and Legacy Services, page 1-15

Hardware and Software Compatibility

For a complete list of supported hardware and software, see Cisco ASA Compatibility:

VPN Compatibility

See Supported VPN Platforms, Cisco ASA Series:
New Features

- New Features in ASA 9.3(3), page 1-2
- New Features in ASA 9.3(2.200), page 1-2
- New Features in ASA 9.3(2.200), page 1-2
- New Features in ASA 9.3(1), page 1-6

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

New Features in ASA 9.3(3)

Released: April 22, 2015

The following table lists the new features for ASA 9.3(3).

<table>
<thead>
<tr>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform Features</strong></td>
</tr>
</tbody>
</table>
| Show invalid usernames in syslog messages | You can now show invalid usernames in syslog messages for unsuccessful login attempts. The default setting is to hide usernames when the username is invalid or if the validity is unknown. If a user accidentally types a password instead of a username, for example, then it is more secure to hide the “username” in the resultant syslog message. You might want to show invalid usernames to help with troubleshooting login issues.
We introduced the following command: \texttt{no logging hide username} 
This feature is not available in 9.4(1). |

New Features in ASA 9.3(2.200)

Released: December 18, 2014

The following table lists the new features for ASA Version 9.3(2.200).

Note: This release supports only the ASAv.

<table>
<thead>
<tr>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform Features</strong></td>
</tr>
<tr>
<td>ASAv with KVM and Virtio</td>
</tr>
</tbody>
</table>
New Features in ASA 9.3(2)

Released: December 18, 2014

The following table lists the new features for ASA Version 9.3(2).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform Features</strong></td>
<td></td>
</tr>
<tr>
<td>ASA 5506-X</td>
<td>We introduced the ASA 5506-X. We introduced or modified the following commands: <code>service sw-reset-button</code>, <code>upgrade rommon</code>, <code>show environment temperature accelerator</code></td>
</tr>
<tr>
<td>ASA FirePOWER software module for the ASA 5506-X</td>
<td>You can configure ASA FirePOWER on the ASA 5506-X using ASDM; a separate FireSIGHT Management Center is not required, although you can use one instead of ASDM. <strong>Note:</strong> This feature requires ASA 7.3(3).</td>
</tr>
<tr>
<td>ASA FirePOWER passive monitor-only mode using traffic redirection interfaces</td>
<td>You can now configure a traffic forwarding interface to send traffic to the module instead of using a service policy. In this mode, neither the module nor the ASA affects the traffic. We fully supported the following command: <code>traffic-forward sfr monitor-only</code>. You can configure this in CLI only.</td>
</tr>
</tbody>
</table>
| Mixed level SSPs in the ASA 5585-X | You can now use the following mixed level SSPs in the ASA 5585-X:  
  - ASA SSP-10/ASA FirePOWER SSP-40
  - ASA SSP-20/ASA FirePOWER SSP-60
Requirements: ASA SSP in slot 0, ASA FirePOWER SSP in slot 1 |
| ASA REST API 1.0.1 | A REST API was added to support configuring and managing major functions of the ASA. We introduced or modified the following commands: `rest-api image`, `rest-api agent`, `show rest-api agent`, `debug rest-api`, `show version` |
| Support for ASA image signing and verification | ASA images are now signed using a digital signature. The digital signature is verified after the ASA is booted. We introduced the following commands: `copy/noverify`, `verify/image-signature`, `show software authenticity keys`, `show software authenticity file`, `show software authenticity running`, `show software authenticity development`, `show software authenticity key add special`, `show software authenticity key revoke special` |
| Accelerated security path load balancing | The accelerated security path (ASP) load balancing mechanism reduces packet drop and improves throughput by allowing multiple cores of the CPU to receive packets from an interface receive ring and work on them independently. We introduced the following command: `asp load-balance per-packet-auto` |

**Firewall Features**
New Features

Configuration session for editing ACLs and objects. You can now edit ACLs and objects in an isolated configuration session. You can also forward reference objects and ACLs, that is, configure rules and access groups for objects or ACLs that do not yet exist.

Forward referencing of objects and ACLs in access rules. We introduced the following commands: `clear configuration session`, `clear session`, `configure session`, `forward-reference`, `show configuration session`.

SIP support for Trust Verification Services, NAT66, CUCM 10.5, and model 8831 phones. You can now configure Trust Verification Services servers in SIP inspection. You can also use NAT66. SIP inspection has been tested with CUCM 10.5.

Unified Communications support for CUCM 10.5. SIP and SCCP inspections were tested and verified with Cisco Unified Communications Manager 10.5.

Remote Access Features

Browser support for Citrix VDI. We now support an HTML 5-based browser solution for accessing the Citrix VDI, without requiring the Citrix Receiver client on the desktop.

Clientless SSL VPN for Mac OSX 10.9. We now support Clientless SSL VPN features such as the rewriter, smart tunnels, and plugins on all browsers that are supported on Mac OSX 10.9.

Interoperability with standards-based, third-party, IKEv2 remote access clients. We now support VPN connectivity via standards-based, third-party, IKEv2 remote-access clients (in addition to AnyConnect). Authentication support includes preshared keys, certificates, and user authentication via the Extensible Authentication Protocol (EAP).

We introduced or modified the following commands: `ikev2 remote-authentication`, `ikev2 local-authentication`, `clear vpn-sessiondb`, `show vpn-sessiondb`, `vpn-sessiondb logoff`.

Transport Layer Security (TLS) version 1.2 support. We now support TLS version 1.2 for secure message transmission for ASDM, Clientless SSVPN, and AnyConnect VPN.

We introduced or modified the following commands: `ssl client-version`, `ssl server-version`, `ssl cipher`, `ssl trust-point`, `ssl dh-group`, `show ssl`, `show ssl cipher`, `show vpn-sessiondb`.

We deprecated the following command: `ssl encryption`.

AnyConnect 4.0 support for TLS version 1.2. AnyConnect 4.0 now supports TLS version 1.2 with the following four additional cipher suites: DHE-RSA-AES256-SHA256, DHE-RSA-AES128-SHA256, AES256-SHA256, and AES128-SHA256.
Cisco Smart Software Licensing for the ASAv

Smart Software Licensing lets you purchase and manage a pool of licenses. Unlike PAK licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAvs without having to manage each unit’s license key. Smart Software Licensing also lets you see your license usage and needs at a glance.

We introduced the following commands: clear configure license, debug license agent, feature tier, http-proxy, license smart, license smart deregister, license smart register, license smart renew, show license, show running-config license, throughput level

High Availability Features

Lock configuration changes on the standby unit or standby context in a failover pair

You can now lock configuration changes on the standby unit (Active/Standby failover) or the standby context (Active/Active failover) so you cannot make changes on the standby unit outside normal configuration syncing.

We introduced the following command: failover standby config-lock

ASA clustering inter-site deployment in transparent mode with the ASA cluster firewalls between inside networks

You can now deploy a cluster in transparent mode between inside networks and the gateway router at each site (AKA East-West insertion), and extend the inside VLANs between sites. We recommend using Overlay Transport Virtualization (OTV), but you can use any method that ensures that the overlapping MAC Addresses and IP addresses of the gateway router do not leak between sites. Use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide the same virtual MAC and IP addresses to the gateway routers.

Interface Features

Traffic Zones

You can group interfaces together into a traffic zone to accomplish traffic load balancing (using Equal Cost Multi-Path (ECMP) routing), route redundancy, and asymmetric routing across multiple interfaces.

Note: You cannot apply a security policy to a named zone; the security policy is interface-based. When interfaces in a zone are configured with the same access rule, NAT, and service policy, then load-balancing and asymmetric routing operate correctly.

We introduced or modified the following commands: zone, zone-member, show running-config zone, clear configure zone, show zone, show asp table zone, show nameif zone, show conn long, show local-host zone, show route zone, show asp table routing, clear conn zone, clear local-host zone

Routing Features
New Features in ASA 9.3(1)

Released: July 24, 2014

The following table lists the new features for ASA Version 9.3(1).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP support for IPv6</td>
<td>We added support for IPv6. We introduced or modified the following commands: <code>address-family ipv6</code>, <code>bgp router-id</code>, <code>ipv6 prefix-list</code>, <code>ipv6 prefix-list description</code>, <code>ipv6 prefix-list sequence-number</code>, <code>match ipv6 next-hop</code>, <code>match ipv6 route-source</code>, <code>match ipv6-address prefix-list</code>, <code>set ipv6-address prefix-list</code>, <code>set ipv6 next-hop</code>, <code>set ipv6 next-hop peer-address</code></td>
</tr>
</tbody>
</table>

Monitoring Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP MIBs and traps</td>
<td>The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the new ASA 5506-X. The ASA 5506-X have been added as new products to the SNMP sysObjectID OID and entPhysicalVendorType OID. The ASA now supports the CISCO-CONFIG-MAN-MIB, which enables you to do the following: • Know which commands have been entered for a specific configuration. • Notify the NMS when a change has occurred in the running configuration. • Track the time stamps associated with the last time that the running configuration was changed or saved. • Track other changes to commands, such as terminal details and command sources. We modified the following command: <code>snmp-server enable traps</code></td>
</tr>
</tbody>
</table>

Showing route summary information for troubleshooting | The `show route-summary` command output has been added to the `show tech-support detail` command. |

Management Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System backup and restore</td>
<td>We now support complete system backup and restoration using the CLI. We introduced the following commands: <code>backup</code>, <code>restore</code></td>
</tr>
</tbody>
</table>

New Features in ASA 9.3(2) (continued)

Table 1-3  New Features for ASA Version 9.3(2) (continued)
### Table 1-4  New Features for ASA Version 9.3(1)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Features</strong></td>
<td></td>
</tr>
<tr>
<td>SIP, SCCP, and TLS Proxy support for IPv6</td>
<td>You can now inspect IPv6 traffic when using SIP, SCCP, and TLS Proxy (using SIP or SCCP). We did not modify any commands.</td>
</tr>
<tr>
<td>Support for Cisco Unified Communications</td>
<td>The ASA now interoperates with Cisco Unified Communications Manager Version 8.6 (including SCCPv21 support). We did not modify any commands.</td>
</tr>
<tr>
<td>Manager 8.6</td>
<td></td>
</tr>
<tr>
<td>Transactional Commit Model on rule engine</td>
<td>When enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. We introduced the following commands: <em>asp rule-engine transactional-commit</em>, <em>show running-config asp rule-engine transactional-commit</em>, <em>clear configure asp rule-engine transactional-commit</em></td>
</tr>
<tr>
<td>for access groups and NAT</td>
<td></td>
</tr>
<tr>
<td><strong>Remote Access Features</strong></td>
<td></td>
</tr>
<tr>
<td>XenDesktop 7 Support for clientless SSL VPN</td>
<td>We added support for XenDesktop 7 to clientless SSL VPN. When creating a bookmark with auto sign-on, you can now specify a landing page URL or a Control ID. We did not modify any commands.</td>
</tr>
<tr>
<td>AnyConnect Custom Attribute Enhancements</td>
<td>Custom attributes define and configure AnyConnect features that have not been incorporated into the ASA, such as Deferred Upgrade. Custom attribute configuration has been enhanced to allow multiple values and longer values, and now requires a specification of their type, name and value. They can now be added to Dynamic Access Policies as well as Group Policies. Previously defined custom attributes will be updated to this enhanced configuration format upon upgrade to 9.3.x. We introduced or modified the following commands: <em>anyconnect-custom-attr</em>, <em>anyconnect-custom-data</em>, and <em>anyconnect-custom</em></td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Identity Extensions (ACIDex) for Desktop Platforms</td>
<td>ACIDex, also known as AnyConnect Endpoint Attributes or Mobile Posture, is the method used by the AnyConnect VPN client to communicate posture information to the ASA. Dynamic Access Polices use these endpoint attributes to authorize users. The AnyConnect VPN client now provides Platform identification for the desktop operating systems (Windows, Mac OS X, and Linux) and a pool of MAC Addresses which can be used by DAPs. We did not modify any commands.</td>
</tr>
</tbody>
</table>
| TrustSec SGT Assignment for VPN | TrustSec Security Group Tags (SGT) can now be added to the SGT-IP table on the ASA when a remote user connects. We introduced the following new command: `security-group-tag value`

### High Availability Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Improved support for monitoring module health in clustering | We added improved support for monitoring module health in clustering. We modified the following command: `show cluster info health`
| Disable health monitoring of a hardware module | By default, the ASA monitors the health of an installed hardware module such as the ASA FirePOWER module. If you do not want a hardware module failure to trigger failover, you can disable module monitoring. We modified the following command: `monitor-interface service-module`

### Platform Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| ASP Load Balancing | The new `auto` option in the `asp load-balance per-packet` command enables the ASA to adaptively switch ASP load balancing per-packet on and off on each interface receive ring. This automatic mechanism detects whether or not asymmetric traffic has been introduced and helps avoid the following issues:  
  - Overruns caused by sporadic traffic spikes on flows  
  - Overruns caused by bulk flows oversubscribing specific interface receive rings  
  - Overruns caused by relatively heavily overloaded interface receive rings, in which a single core cannot sustain the load  
We introduced or modified the following commands: `asp load-balance per-packet auto`, `show asp load-balance per-packet`, `show asp load-balance per-packet history`, and `clear asp load-balance history`
| SNMP MIBs | The CISCO-REMOTE-ACCESS-MONITOR-MIB now supports the ASASM. |

### Interface Features
Table 1-4  New Features for ASA Version 9.3(1) (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent mode bridge group maximum increased to 250</td>
<td>The bridge group maximum was increased from 8 to 250 bridge groups. You can configure up to 250 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group. We modified the following commands: <code>interface bvi</code>, <code>bridge-group</code></td>
</tr>
</tbody>
</table>

Routing Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP support for ASA clustering</td>
<td>We added support for BGP with ASA clustering. We introduced the following new command: <code>bgp router-id clusterpool</code></td>
</tr>
<tr>
<td>BGP support for nonstop forwarding</td>
<td>We added support for BGP Nonstop Forwarding. We introduced the following new commands: <code>bgp graceful-restart</code>, <code>neighbor ha-mode graceful-restart</code></td>
</tr>
<tr>
<td>BGP support for advertised maps</td>
<td>We added support for BGPv4 advertised map. We introduced the following new command: <code>neighbor advertise-map</code></td>
</tr>
<tr>
<td>OSPF Support for Non-Stop Forwarding (NSF)</td>
<td>OSPFv2 and OSPFv3 support for NSF was added. We added the following commands: <code>capability</code>, <code>nsf cisco</code>, <code>nsf cisco helper</code>, <code>ietf</code>, <code>ietf helper</code>, <code>ietf helper strict-lsa-checking</code>, <code>graceful-restart</code>, <code>graceful-restart helper</code>, <code>graceful-restart helper strict-lsa-checking</code></td>
</tr>
</tbody>
</table>

AAA Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Security Group Tag Imposition</td>
<td>You can now use security group tagging combined with Ethernet tagging to enforce policies. SGT plus Ethernet Tagging, also called Layer 2 SGT Imposition, enables the ASA to send and receive security group tags on Gigabit Ethernet interfaces using Cisco proprietary Ethernet framing (Ether Type 0x8909), which allows the insertion of source security group tags into plain-text Ethernet frames. We introduced or modified the following commands: <code>cts manual</code>, <code>policy static sgt</code>, <code>propagate sgt</code>, <code>cts role-based sgt-map</code>, <code>show cts sgt-map</code>, <code>packet-tracer</code>, <code>capture</code>, <code>show capture</code>, <code>show asp drop</code>, <code>show asp table classify</code>, <code>show running-config all</code>, <code>clear configure all</code>, and <code>write memory</code></td>
</tr>
<tr>
<td>Removal of AAA Windows NT domain authentication</td>
<td>We removed NTLM support for remote access VPN users. We deprecated the following command: <code>aaa-server protocol nt</code></td>
</tr>
</tbody>
</table>
Firewall Functional Overview

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

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

- Security Policy Overview, page 1-10
- Firewall Mode Overview, page 1-12
- Stateful Inspection Overview, page 1-13

Security Policy Overview

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

- Permitting or Denying Traffic with Access Lists, page 1-11
- Applying NAT, page 1-11
- Protecting from IP Fragments, page 1-11
- Applying HTTP, HTTPS, or FTP Filtering, page 1-11
- Applying Application Inspection, page 1-11
- Sending Traffic to Supported Hardware or Software Modules, page 1-11
- Applying QoS Policies, page 1-12
- Applying Connection Limits and TCP Normalization, page 1-12

---

Table 1-4 New Features for ASA Version 9.3(1) (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Aggregated Traffic for Physical Interfaces</td>
<td>The <code>show traffic</code> command output has been updated to include aggregated traffic for physical interfaces information. To enable this feature, you must first enter the <code>sysopt traffic detailed-statistics</code> command.</td>
</tr>
</tbody>
</table>
• Enabling Threat Detection, page 1-12

Permitting or Denying Traffic with Access Lists

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

Applying NAT

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

Protecting from IP Fragments

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

Applying HTTP, HTTPS, or FTP Filtering

Although you can use access lists to prevent outbound access to specific websites or FTP servers, configuring and managing web usage this way is not practical because of the size and dynamic nature of the Internet.

You can configure Cloud Web Security on the ASA, or install an ASA module that provides URL and other filtering services, such as ASA CX or ASA FirePOWER. You can also use the ASA in conjunction with an external product such as the Cisco Web Security Appliance (WSA).

Applying Application Inspection

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

Sending Traffic to Supported Hardware or Software Modules

Some ASA models allow you to configure software modules, or to insert hardware modules into the chassis, to provide advanced services. These modules provide additional traffic inspection and can block traffic based on your configured policies. You can send traffic to these modules to take advantage of these advanced services.
Applying QoS Policies

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

Applying Connection Limits and TCP Normalization

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

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

Enabling Threat Detection

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

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

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

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

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

Firewall Mode Overview

The ASA runs in two different firewall modes:

- Routed
- Transparent

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

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

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.

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

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

The session management path is responsible for the following tasks:

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

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

Note

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

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

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

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

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

VPN Functional Overview

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

The ASA performs the following functions:

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

The ASA invokes various standard protocols to accomplish these functions.

Security Context Overview

You can partition a single ASA into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management; however, some features are not supported. See the feature chapters for more information.

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

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

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

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

Special and Legacy Services

For some services, documentation is located outside of the main configuration guides and online help. For a complete list of guides, see:

http://www.cisco.com/go/asadocs
- Special Services Guides, page 1-15
- Legacy Services Guide, page 1-15

Special Services Guides

Special services allow the ASA to interoperate with other Cisco products; for example, by providing a security proxy for phone services (Unified Communications), or by providing Botnet traffic filtering in conjunction with the dynamic database from the Cisco update server, or by providing WCCP services for the Cisco Web Security Appliance. Some of these special services are covered in separate guides.

Legacy Services Guide

Legacy services are still supported on the ASA, however there may be better alternative services that you can use instead. Legacy services are covered in a separate guide.
Getting Started

This chapter describes how to get started with your Cisco ASA.

- Access the Console for Command-Line Interface, page 2-1
- Configure ASDM Access, page 2-6
- Start ASDM, page 2-11
- Factory Default Configurations, page 2-13
- Work with the Configuration, page 2-17
- Apply Configuration Changes to Connections, page 2-21
- Reload the ASA, page 2-22

Access the Console for Command-Line Interface

For initial configuration, access the CLI directly from the console port. Later, you can configure remote access using Telnet or SSH according to Chapter 35, “Management Access.” If your system is already in multiple context mode, then accessing the console port places you in the system execution space.

Note

For ASAv console access, see the ASAv quick start guide.

- Access the Appliance Console, page 2-1
- Access the ASA Services Module Console, page 2-2

Access the Appliance Console

Follow these steps to access the appliance console.

Procedure

Step 1
Connect a computer to the console port using the provided console cable, and connect to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

See the hardware guide for your ASA for more information about the console cable.

Step 2
Press the Enter key to see the following prompt:
Access the ASA Services Module Console

For initial configuration, access the command-line interface by connecting to the switch (either to the console port or remotely using Telnet or SSH) and then connecting to the ASASM. This section describes how to access the ASASM CLI.

- **About Connection Methods**, page 2-2
- **Log Into the ASA Services Module**, page 2-3
- **Log Out of a Console Session**, page 2-5
- **Kill an Active Console Connection**, page 2-5
- **Log Out of a Telnet Session**, page 2-6

**About Connection Methods**

From the switch CLI, you can use two methods to connect to the ASASM:

- Virtual console connection—Using the `service-module session` command, you create a virtual console connection to the ASASM, with all the benefits and limitations of an actual console connection.
Benefits include:
- The connection is persistent across reloads and does not time out.
- You can stay connected through ASASM reloads and view startup messages.
- You can access ROMMON if the ASASM cannot load the image.
- No initial password configuration is required.

Limitations include:
- The connection is slow (9600 baud).
- You can only have one console connection active at a time.
- You cannot use this command in conjunction with a terminal server where Ctrl-Shift-6, x is the escape sequence to return to the terminal server prompt. Ctrl-Shift-6, x is also the sequence to escape the ASASM console and return to the switch prompt. Therefore, if you try to exit the ASASM console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the switch, the ASASM console session is still active; you can never exit to the switch prompt. You must use a direct serial connection to return the console to the switch prompt. In this case, either change the terminal server or switch escape character in Cisco IOS software, or use the Telnet session command instead.

| Note | Because of the persistence of the console connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection. |

- Telnet connection—Using the session command, you create a Telnet connection to the ASASM.

| Note | You cannot connect using this method for a new ASASM; this method requires you to configure a Telnet login password on the ASASM (there is no default password). After you set a password using the passwd command, you can use this method. |

Benefits include:
- You can have multiple sessions to the ASASM at the same time.
- The Telnet session is a fast connection.

Limitations include:
- The Telnet session is terminated when the ASASM reloads, and can time out.
- You cannot access the ASASM until it completely loads; you cannot access ROMMON.
- You must first set a Telnet login password; there is no default password.

### Log Into the ASA Services Module

For initial configuration, access the command-line interface by connecting to the switch (either to the switch console port or remotely using Telnet or SSH) and then connecting to the ASASM.

If your system is already in multiple context mode, then accessing the ASASM from the switch places you in the system execution space.

Later, you can configure remote access directly to the ASASM using Telnet or SSH.
Procedure

Step 1
From the switch, perform one of the following:

- Available for initial access—From the switch CLI, enter this command to gain console access to the ASASM:

  ```
  service-module session [switch (1 | 2)] slot number
  ```

  Example:

  ```
  Router# service-module session slot 3
ciscoasa>
  ```

  For a switch in a VSS, enter the `switch` argument.

  To view the module slot numbers, enter the `show module` command at the switch prompt.

  You access user EXEC mode.

- Available after you configure a login password—From the switch CLI, enter this command to Telnet to the ASASM over the backplane:

  ```
  session [switch (1 | 2)] slot number processor 1
  ```

  You are prompted for the login password:

  ```
  ciscoasa passwd:
  ```

  Example:

  ```
  Router# session slot 3 processor 1
ciscoasa passwd: cisco
ciscoasa>
  ```

  For a switch in a VSS, enter the `switch` argument.

  The `session slot processor 0` command, which is supported on other services modules, is not supported on the ASASM; the ASASM does not have a processor 0.

  To view the module slot numbers, enter the `show module` command at the switch prompt.

  Enter the login password to the ASASM. Set the password using the `passwd` command. There is no default password.

  You access user EXEC mode.

Step 2
Access privileged EXEC mode, which is the highest privilege level:

```
enable
```

Example:

```
ciscoasa> enable
Password:
ciscoasa#
```

Enter the enable password at the prompt. By default, the password is blank.

To exit privileged EXEC mode, enter the `disable`, `exit`, or `quit` command.

Step 3
Access global configuration mode:

```
configure terminal
```
To exit global configuration mode, enter the **disable**, **exit**, or **quit** command.

### Related Topics
- Guidelines for Management Access, page 35-1.
- Set the Hostname, Domain Name, and the Enable and Telnet Passwords, page 14-1

### Log Out of a Console Session

If you do not log out of the ASASM, the console connection persists; there is no timeout. To end the ASASM console session and access the switch CLI, perform the following steps.

To kill another user’s active connection, which may have been unintentionally left open, see **Kill an Active Console Connection**, page 2-5.

**Procedure**

**Step 1**

To return to the switch CLI, type the following:

```
Ctrl-Shift-6, x
```

You return to the switch prompt:

```
asasm# [Ctrl-Shift-6, x]
```

```
Router#
```

**Note**

Shift-6 on US and UK keyboards issues the caret (^) character. If you have a different keyboard and cannot issue the caret (^) character as a standalone character, you can temporarily or permanently change the escape character to a different character. Use the `terminal escape-character ascii_number` command (to change for this session) or the `default escape-character ascii_number` command (to change permanently). For example, to change the sequence for the current session to `Ctrl-w, x`, enter `terminal escape-character 23`.

### Kill an Active Console Connection

Because of the persistence of a console connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection.

**Procedure**

**Step 1**

From the switch CLI, show the connected users using the `show users` command. A console user is called “con”. The Host address shown is 127.0.0.slot0, where `slot` is the slot number of the module.

```
Router# show users
```

For example, the following command output shows a user “con” on line 0 on a module in slot 2:

```
Line   User        Host(s)         Idle  Location
```
Step 2 To clear the line with the console connection, enter the following command:

```
Router# clear line number
```

For example:

```
Router# clear line 0
```

Log Out of a Telnet Session

To end the Telnet session and access the switch CLI, perform the following steps.

**Procedure**

**Step 1** To return to the switch CLI, type `exit` from the ASASM privileged or user EXEC mode. If you are in a configuration mode, enter `exit` repeatedly until you exit the Telnet session.

You return to the switch prompt:

```
asasm# exit
Router#
```

**Note** You can alternatively escape the Telnet session using the escape sequence `Ctrl-Shift-6, x`; this escape sequence lets you resume the Telnet session by pressing the `Enter` key at the switch prompt. To disconnect your Telnet session from the switch, enter `disconnect` at the switch CLI. If you do not disconnect the session, it will eventually time out according to the ASASM configuration.

Configure ASDM Access

This section describes how to access ASDM with a default configuration and how to configure access if you do not have a default configuration.

- Use the Factory Default Configuration for ASDM Access (Appliances, ASAv), page 2-6
- Customize ASDM Access for Appliances and the ASAv, page 2-7
- Configure ASDM Access for the ASA Services Module, page 2-9

Use the Factory Default Configuration for ASDM Access (Appliances, ASAv)

With a factory default configuration, ASDM connectivity is pre-configured with default network settings.
Configure ASDM Access

Procedure

Step 1  Connect to ASDM using the following interface and network settings:

- The management interface depends on your model:
  - ASA 5506-X—The interface to which you connect to ASDM is Management 1/1.
  - ASA 5512-X and higher—The interface to which you connect to ASDM is Management 0/0.
  - ASAv—The interface to which you connect to ASDM is Management 0/0.
- The default management address is:
  - ASAv—You set the management interface IP address during deployment.
- The clients allowed to access ASDM:
  - ASA appliances—Clients must be on the 192.168.1.0/24 network. The default configuration enables DHCP so that your management station can be assigned an IP address in this range.
  - ASAv—You set the management client IP address during deployment. The ASAv does not act as the DHCP server for connected clients.

Note  If you change to multiple context mode, you can access ASDM from the admin context using the network settings above.

Related Topics
- Factory Default Configurations, page 2-13
- Enable or Disable Multiple Context Mode, page 6-15
- Start ASDM, page 2-11

Customize ASDM Access for Appliances and the ASAv

Use this procedure if one or more of the following conditions applies:

- You do not have a factory default configuration
- You want to change the management IP address
- You want to change to transparent firewall mode
- You want to change to multiple context mode

For routed, single mode, for quick and easy ASDM access, we recommend applying the factory default configuration with the option to set your own management IP address. Use the procedure in this section only if you have special needs such as setting transparent or multiple context mode, or if you have other configuration that you need to preserve.

Note  For the ASAv, you can configure transparent mode when you deploy (in 9.3(2) and later), so this procedure is primarily useful after you deploy if you need to clear your configuration, for example.
Procedure

Step 1  Access the CLI at the console port.

Step 2  (Optional) Enable transparent firewall mode:
This command clears your configuration.
firewall transparent

Step 3  Configure the Management interface:
```plaintext
interface management id
  nameif name
  security-level level
  no shutdown
  ip address ip_address mask
```
Example:
```plaintext
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```
The `security-level` is a number between 1 and 100, where 100 is the most secure.

Step 4  (For directly-connected management hosts) Set the DHCP pool for the management network:
```plaintext
dhcpd address ip_address-ip_address
  interface_name

dhcpd enable interface_name
```
Example:
```plaintext
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management

ciscoasa(config)# dhcpd enable management
```
Make sure you do not include the Management address in the range.

Step 5  (For remote management hosts) Configure a route to the management hosts:
```plaintext
route management_ifc management_host_ip mask gateway_ip
```
Example:
```plaintext
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

Step 6  Enable the HTTP server for ASDM:
```plaintext
http server enable
```

Step 7  Allow the management host(s) to access ASDM:
```plaintext
http ip_address mask interface_name
```
Example:
```plaintext
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

Step 8  Save the configuration:
```plaintext
write memory
```

Step 9  (Optional) Set the mode to multiple mode:
mode multiple

When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASA.

Examples
The following configuration converts the firewall mode to transparent mode, configures the Management 0/0 interface, and enables ASDM for a management host:

```
firwall transparent
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

Related Topics
- Restore the Factory Default Configuration, page 2-13
- Set the Firewall Mode, page 5-9
- Access the Appliance Console, page 2-1
- Start ASDM, page 2-11
- Chapter 6, “Multiple Context Mode.”

Configure ASDM Access for the ASA Services Module

Because the ASASM does not have physical interfaces, it does not come pre-configured for ASDM access; you must configure ASDM access using the CLI on the ASASM. To configure the ASASM for ASDM access, perform the following steps.

Before You Begin
Assign a VLAN interface to the ASASM according to ASASM quick start guide.

Procedure

**Step 1**  Connect to the ASASM and access global configuration mode.

**Step 2**  (Optional) Enable transparent firewall mode:

```
firwall transparent
```

This command clears your configuration.

**Step 3**  Do one of the following to configure a management interface, depending on your mode:

- Routed mode—Configure an interface in routed mode:

```
interface vlan number
  ip address ip_address [mask]
```
nameif name
security-level level

Example:
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100

The security-level is a number between 1 and 100, where 100 is the most secure.

- Transparent mode—Configure a bridge virtual interface and assigns a management VLAN to the bridge group:

  interface bvi number
    ip address ip_address [mask]
  
  interface vlan number
    bridge-group bvi_number
    nameif name
    security-level level

Example:
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100

The security-level is a number between 1 and 100, where 100 is the most secure.

Step 4 (For directly-connected management hosts) Enable DHCP for the management host on the management interface network:

dhcpd address ip_address-ip_address
interface_name
dhcpd enable interface_name

Example:
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside

Make sure you do not include the management address in the range.

Step 5 (For remote management hosts) Configure a route to the management hosts:

route management_ifc management_host_ip mask gateway_ip

Example:
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50

Step 6 Enable the HTTP server for ASDM:

http server enable

Step 7 Allow the management host to access ASDM:

http ip_address mask interface_name

Example:
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management

**Step 8**  
Save the configuration:  
```bash
write memory
```

**Step 9**  
(Optional) Set the mode to multiple mode:  
```bash
mode multiple
```

When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASASM.

---

**Examples**

The following routed mode configuration configures the VLAN 1 interface and enables ASDM for a management host:

```bash
interface vlan 1
    nameif inside
    ip address 192.168.1.1 255.255.255.0
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

The following configuration converts the firewall mode to transparent mode, configures the VLAN 1 interface and assigns it to BVI 1, and enables ASDM for a management host:

```bash
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

**Related Topics**

- Access the ASA Services Module Console, page 2-2
- Chapter 6, “Multiple Context Mode.”
- Set the Firewall Mode, page 5-9

---

**Start ASDM**

You can start ASDM using two methods:

- **ASDM-IDM Launcher**—The Launcher is an application downloaded from the ASA using a web browser that you can use to connect to any ASA IP address. You do not need to re-download the launcher if you want to connect to other ASAs. The Launcher also lets you run a virtual ASDM in Demo mode using files downloaded locally.
Java Web Start—For each ASA that you manage, you need to connect with a web browser and then save or launch the Java Web Start application. You can optionally save the shortcut to your computer; however you need separate shortcuts for each ASA IP address.

Within ASDM, you can choose a different ASA IP address to manage; the difference between the Launcher and Java Web Start functionality rests primarily in how you initially connect to the ASA and launch ASDM.

This section describes how to connect to ASDM initially, and then launch ASDM using the Launcher or the Java Web Start.

Procedure

### Step 1
On the computer that you specified as the ASDM client, enter the following URL:

https://asa_ip_address/admin

The ASDM launch page appears with the following buttons:

- Install ASDM Launcher and Run ASDM
- Run ASDM
- Run Startup Wizard

### Step 2
To download the Launcher:

a. Click Install ASDM Launcher and Run ASDM.

b. Leave the username and password fields empty (for a new installation), and click OK. With no HTTPS authentication configured, you can gain access to ASDM with no username and the enable password, which is blank by default. Note: If you enabled HTTPS authentication, enter your username and associated password.

c. Save the installer to your computer, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

d. Enter the management IP address, leave the username and password blank (for a new installation), and then click OK. Note: If you enabled HTTPS authentication, enter your username and associated password.

### Step 3
To use Java Web Start:

a. Click Run ASDM or Run Startup Wizard.

b. Save the shortcut to your computer when prompted. You can optionally open it instead of saving it.

c. Start Java Web Start from the shortcut.

d. Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

e. Leave the username and password blank (for a new installation), and then click OK. Note: If you enabled HTTPS authentication, enter your username and associated password.
Factory Default Configurations

The factory default configuration is the configuration applied by Cisco to new ASAs.

- **ASA appliances**—The factory default configuration configures an interface for management so that you can connect to it using ASDM, with which you can then complete your configuration.

- **ASAv**—As part of deployment, the deployment configuration (the initial virtual deployment settings) configures an interface for management so that you can connect to it using ASDM, with which you can then complete your configuration. You can also configure failover IP addresses. You can also apply a “factory default” configuration if desired.

- **ASASM**—No default configuration. See Access the ASA Services Module Console, page 2-2 to start configuration.

For appliances, the factory default configuration is available only for routed firewall mode and single context mode. For the ASAv, you can choose transparent or routed mode at deployment (9.3(2) and later).

**Note**

In addition to the image files and the (hidden) default configuration, the following folders and files are standard in flash memory: log/, crypto_archive/, and coredumpinfo/coredump.cfg. The date on these files may not match the date of the image files in flash memory. These files aid in potential troubleshooting; they do not indicate that a failure has occurred.

- Restore the Factory Default Configuration, page 2-13
- Restore the ASAv Deployment Configuration, page 2-14
- ASA Appliance Default Configuration, page 2-15
- ASAv Deployment Configuration, page 2-15

Restore the Factory Default Configuration

This section describes how to restore the factory default configuration. For the ASAv, this procedure erases the deployment configuration and applies the same factory default configuration as for the ASA appliances.

**Note**

On the ASASM, restoring the factory default configuration simply erases the configuration; there is no factory default configuration.

**Before You Begin**

This feature is available only in routed firewall mode; transparent mode does not support IP addresses for interfaces. In addition, this feature is available only in single context mode; an ASA with a cleared configuration does not have any defined contexts to configure automatically using this feature.

**Procedure**

**Step 1**

Restore the factory default configuration:

```
configure factory-default [ip_address [mask]]
```

Example:
If you specify the `ip_address`, then you set the inside or management interface IP address, depending on your model, instead of using the default IP address of 192.168.1.1. The `http` command uses the subnet you specify. Similarly, the `dhcpd address` command range consists of addresses within the subnet that you specify.

This command also clears the `boot system` command, if present, along with the rest of the configuration. The `boot system` command lets you boot from a specific image, including an image on the external flash memory card. The next time you reload the ASA after restoring the factory configuration, it boots from the first image in internal flash memory; if you do not have an image in internal flash memory, the ASA does not boot.

**Step 2**  
Save the default configuration to flash memory:

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

This command saves the running configuration to the default location for the startup configuration, even if you previously configured the `boot config` command to set a different location; when the configuration was cleared, this path was also cleared.

---

**Restore the ASAv Deployment Configuration**

This section describes how to restore the ASAv deployment configuration.

**Procedure**

**Step 1**  
For failover, power off the standby unit.

To prevent the standby unit from becoming active, you must power it off. If you leave it on, when you erase the active unit configuration, then the standby unit becomes active. When the former active unit reloads and reconnects over the failover link, the old configuration will sync from the new active unit, wiping out the deployment configuration you wanted.

**Step 2**  
Restore the deployment configuration after you reload. For failover, enter this command on the active unit:

```
ciscoasa(config)# write erase
```

**Note**  
The ASAv boots the current running image, so you are not reverted to the original boot image. To use the original boot image, see the `boot image` command.

Do not save the configuration.

**Step 3**  
Reload the ASAv and load the deployment configuration:

```
ciscoasa(config)# reload
```

**Step 4**  
For failover, power on the standby unit.

After the active unit reloads, power on the standby unit. The deployment configuration will sync to the standby unit.
ASA Appliance Default Configuration

The default factory configuration for the ASA appliances configures the following:

- **Management interface:**
  - ASA 5506-X—Management 1/1 (management).
  - ASA 5512-X and higher—Management 0/0 (management).
- **IP address**—The management address is 192.168.1.1/24.
- **DHCP server**—Enabled for management hosts so that a computer connecting to the management interface receives an address between 192.168.1.2 and 192.168.1.254.
- **ASDM access**—Management hosts allowed.

The configuration consists of the following commands:

```
interface management 0/0
  ! or interface management 1/1
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
  asdm logging informational 100
  asdm history enable
  http server enable
  http 192.168.1.0 255.255.255.0 management
  dhcpd address 192.168.1.2-192.168.1.254 management
  dhcpd lease 3600
  dhcpd ping_timeout 750
  dhcpd enable management
```

ASAv Deployment Configuration

When you deploy the ASAv, you can pre-set many parameters that let you connect to the Management 0/0 interface using ASDM. A typical configuration includes the following settings:

- (9.3(2) and later) Routed or Transparent firewall mode
- Management 0/0 interface:
  - Named “management”
  - IP address or DHCP
  - Security level 0
  - Management-only
- Default route through the management interface
- HTTP server enabled or disabled
- HTTP access for the management host IP address
- (Optional) Failover link IP addresses for GigabitEthernet 0/8, and the Management 0/0 standby IP address
- (9.3(2) and later) DNS server
- (9.3(2) and later) Smart Software Licensing ID token
- (9.3(2) and later) Smart Software Licensing Throughput Level and Standard Feature Tier
Factory Default Configurations

- (9.3(2) and later; Optional) Smart Call Home HTTP Proxy URL and port
- (9.3(2) and later; Optional) SSH management settings:
  - Client IP addresses
  - Local username and password
  - Authentication required for SSH using the LOCAL database
- (9.3(2) and later; Optional) REST API enabled or disabled

Note

To successfully register the ASAv with the Cisco Licensing Authority, the ASAv requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

See the following configuration for a standalone unit:

```plaintext
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address
  management-only
  http server enable
  http management_host_IP mask management
  route management 0.0.0.0 0.0.0.0 gateway_ip 1
  dns server-group DefaultDNS
    name-server ip_address
  call-home
    http-proxy ip_address port port
  license smart
    feature tier standard
    throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
  aaa authentication ssh console LOCAL
  username username password password
  ssh client_IP_address mask management
  rest-api image boot:/path
  rest-api agent
```

See the following configuration for a primary unit in a failover pair:

```plaintext
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address standby standby_ip
  management-only
  route management 0.0.0.0 0.0.0.0 gateway_ip 1
  http server enable
  http management_host_IP mask management
  dns server-group DefaultDNS
    name-server ip_address
  call-home
    http-proxy ip_address port port
  license smart
    feature tier standard
    throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
  aaa authentication ssh console LOCAL
  username username password password
  ssh client_IP_address mask management
  rest-api image boot:/path
  rest-api agent
```
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip

Work with the Configuration

This section describes how to work with the configuration. The ASA loads the configuration from a text file, called the startup configuration. This file resides by default as a hidden file in internal flash memory. You can, however, specify a different path for the startup configuration.

When you enter a command, the change is made only to the running configuration in memory. You must manually save the running configuration to the startup configuration for your changes to remain after a reboot.

The information in this section applies to both single and multiple security contexts, except where noted.

- Save Configuration Changes, page 2-17
- Copy the Startup Configuration to the Running Configuration, page 2-19
- View the Configuration, page 2-19
- Clear and Remove Configuration Settings, page 2-20
- Create Text Configuration Files Offline, page 2-21

Save Configuration Changes

This section describes how to save your configuration.

- Save Configuration Changes in Single Context Mode, page 2-17
- Save Configuration Changes in Multiple Context Mode, page 2-18

Save Configuration Changes in Single Context Mode

To save the running configuration to the startup configuration, perform the following procedure.

Procedure

Step 1

Save the running configuration to the startup configuration:

write memory

Note

The `copy running-config startup-config` command is equivalent to the `write memory` command.
Save Configuration Changes in Multiple Context Mode

You can save each context (and system) configuration separately, or you can save all context configurations at the same time.

- Save Each Context and System Separately, page 2-18
- Save All Context Configurations at the Same Time, page 2-18

Save Each Context and System Separately

Use the following procedure to save the system or context configuration.

Procedure

Step 1
From within the context or the system, save the running configuration to the startup configuration:

```
write memory
```

For multiple context mode, context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server you identified in the context URL, except for an HTTP or HTTPS URL, which do not let you save the configuration to the server.

Note

The `copy running-config startup-config` command is equivalent to the `write memory` command.

Save All Context Configurations at the Same Time

Use the following procedure to save all context configurations at the same time, as well as the system configuration.

Procedure

Step 1
From the system execution space, save the running configuration to the startup configuration for all contexts and the system configuration:

```
write memory all [/noconfirm]
```

If you do not enter the `/noconfirm` keyword, you see the following prompt:

```
Are you sure [Y/N]:
```

After you enter `Y`, the ASA saves the system configuration and each context. Context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server you identified in the context URL, except for an HTTP or HTTPS URL, which do not let you save the configuration to the server.

After the ASA saves each context, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

```
The context 'context a' could not be saved due to Unavailability of resources
```
• For contexts that are not saved because the remote destination is unreachable, the following message appears:
The context ‘context a’ could not be saved due to non-reachability of destination

• For contexts that are not saved because the context is locked, the following message appears:
Unable to save the configuration for the following contexts as these contexts are locked.
context ‘a’, context ‘x’, context ‘z’.

A context is only locked if another user is already saving the configuration or in the process of deleting the context.

• For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:
Unable to save the configuration for the following contexts as these contexts have read-only config-urls:
context ‘a’, context ‘b’, context ‘c’.

• For contexts that are not saved because of bad sectors in the flash memory, the following message appears:
The context ‘context a’ could not be saved due to Unknown errors

Copy the Startup Configuration to the Running Configuration

Use one of the following commands to copy a new startup configuration to the running configuration:

• copy startup-config running-config
Merges the startup configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.

• reload
Reloads the ASA, which loads the startup configuration and discards the running configuration.

• clear configure all and then copy startup-config running-config
Loads the startup configuration and discards the running configuration without requiring a reload.

View the Configuration

The following commands let you view the running and startup configurations:

• show running-config
Views the running configuration.

• show running-config command
Views the running configuration of a specific command.

• show startup-config
Views the startup configuration.

**Clear and Remove Configuration Settings**

To erase settings, enter one of the following commands:

- `clear configure configurationcommand [level2configurationcommand]
  
  Clears all the configuration for a specified command. If you only want to clear the configuration for a specific version of the command, you can enter a value for `level2configurationcommand`. For example, to clear the configuration for all `aaa` commands, enter the following command:
  
  `ciscoasa(config)# clear configure aaa`

  To clear the configuration for only `aaa authentication` commands, enter the following command:
  
  `ciscoasa(config)# clear configure aaa authentication`

- `no configurationcommand [level2configurationcommand] qualifier
  
  Disables the specific parameters or options of a command. In this case, you use the `no` command to remove the specific configuration identified by `qualifier`. For example, to remove a specific `access-list` command, enter enough of the command to identify it uniquely; you may have to enter the entire command:
  
  `ciscoasa(config)# no access-list abc extended permit icmp any any object-group obj_icmp_1`

- `write erase
  
  Erases the startup configuration.

  **Note**  
  For the ASAv, this command restores the deployment configuration after a reload. To erase the configuration completely, use the `clear configure all` command.

- `clear configure all
  
  Erases the running configuration.

  **Note**  
  In multiple context mode, if you enter `clear configure all` from the system configuration, you also remove all contexts and stop them from running. The context configuration files are not erased, and remain in their original location.

  This command also clears the `boot system` command, if present, along with the rest of the configuration. The `boot system` command lets you boot from a specific image, including an image on the external flash memory card. The next time you reload the ASA, it boots from the first image in internal flash memory; if you do not have an image in internal flash memory, the ASA does not boot.
Create Text Configuration Files Offline

This guide describes how to use the CLI to configure the ASA; when you save commands, the changes are written to a text file. Instead of using the CLI, however, you can edit a text file directly on your computer and paste a configuration at the configuration mode command-line prompt in its entirety, or line by line. Alternatively, you can download a text file to the ASA internal flash memory. See Chapter 36, “Software and Configurations,” for information on downloading the configuration file to the ASA.

In most cases, commands described in this guide are preceded by a CLI prompt. The prompt in the following example is “ciscoasa(config)#”:

```
ciscoasa(config)# context a
```

In the text configuration file you are not prompted to enter commands, so the prompt is omitted as follows:

```
context a
```

For additional information about formatting the file, see Appendix 42, “Using the Command-Line Interface.”

Apply Configuration Changes to Connections

When you make security policy changes to the configuration, all new connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. show command output for old connections reflect the old configuration, and in some cases will not include data about the old connections.

For example, if you remove a QoS service-policy from an interface, then re-add a modified version, then the show service-policy command only displays QoS counters associated with new connections that match the new service policy; existing connections on the old policy no longer show in the command output.

To ensure that all connections use the new policy, you need to disconnect the current connections so that they can reconnect using the new policy.

To disconnect connections, enter one of the following commands:

- **clear local-host [ip_address] [all]**
  
  This command reinitializes per-client run-time states such as connection limits and embryonic limits. As a result, this command removes any connection that uses those limits. See the show local-host all command to view all current connections per host.

  With no arguments, this command clears all affected through-the-box connections. To also clear to-the-box connections (including your current management session), use the all keyword. To clear connections to and from a particular IP address, use the ip_address argument.

- **clear conn [all] [protocol {tcp | udp}] [address src_ip[-src_ip] [netmask mask]] [port src_port[-src_port]] [address dest_ip[-dest_ip] [netmask mask]] [port dest_port[-dest_port]]**

  This command terminates connections in any state. See the show conn command to view all current connections.

  With no arguments, this command clears all through-the-box connections. To also clear to-the-box connections (including your current management session), use the all keyword. To clear specific connections based on the source IP address, destination IP address, port, and/or protocol, you can specify the desired options.
Reload the ASA

To reload the ASA, complete the following procedure.

Procedure

Step 1

Reload the ASA:

```
reload
```

Note

In multiple context mode, you can only reload from the system execution space.
Product Authorization Key Licenses

A license specifies the options that are enabled on a given Cisco ASA. This document describes product authorization key (PAK) licenses for all physical ASAs and the ASAv in Version 9.3(1). For the ASAv in Version 9.3(2), see Chapter 4, “Smart Software Licensing for the ASAv.”

- Supported Feature Licenses Per Model, page 3-1
- About PAK Licenses, page 3-20
- Guidelines for PAK Licenses, page 3-28
- Configure PAK Licenses, page 3-29
- Configure a Shared License, page 3-31
- Monitoring PAK Licenses, page 3-38
- History for PAK Licenses, page 3-50

Supported Feature Licenses Per Model

This section describes the licenses available for each model as well as important notes about licenses.

- Licenses Per Model, page 3-1
- License Notes, page 3-15

Licenses Per Model

This section lists the feature licenses available for each model:

- ASA 5506-X, page 3-3
- ASA 5512-X, page 3-4
- ASA 5515-X, page 3-4
- ASA 5525-X, page 3-6
- ASA 5545-X, page 3-6
- ASA 5555-X, page 3-7
- ASA 5585-X with SSP-10, page 3-8
- ASA 5585-X with SSP-20, page 3-9
- ASA 5585-X with SSP-40 and -60, page 3-10
- ASA Services Module, page 3-11
- ASAv10 (9.3(1)), page 3-12
- ASAv30 (9.3(1)), page 3-13

Items that are in *italics* are separate, optional licenses that can replace the Base (or Security Plus, and so on) license version. You can mix and match licenses; for example, the 24 Unified Communications license plus the Strong Encryption license; or the 500 AnyConnect Premium license plus the GTP/GPRS license; or all four licenses together.

---

**Note**

Some features are incompatible with each other. See the individual feature chapters for compatibility information.

If you have a No Payload Encryption model, then some of the features below are not supported. See No Payload Encryption Models, page 3-27 for a list of unsupported features.

For detailed information about licenses, see License Notes, page 3-15.
### ASA 5506-X

**Table 3-1 ASA 5506-X License Features**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
<th>Security Plus License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>No support</td>
<td>No Support</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>20,000</td>
<td>50,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>No support</td>
<td>No support</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td>require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.</td>
<td></td>
</tr>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>No support</td>
<td>No support</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Other VPN Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>10</td>
<td>50</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>No support</td>
<td>No support</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
<td>Opt. lic.: Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>No support</td>
<td>Active/Standby</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>536</td>
<td>636</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
<td>No support</td>
</tr>
<tr>
<td>Clustering</td>
<td>No Support</td>
<td>No Support</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>5</td>
<td>30</td>
</tr>
</tbody>
</table>
ASA 5512-X

Table 3-2  ASA 5512-X License Features

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
<th>Security Plus License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
<td>Optional Time-based license: Available</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>100,000</td>
<td>250,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>No support</td>
<td>No support</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Disabled</td>
<td>Optional license: Available</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2</td>
<td>Optional licenses: 24</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
<td>Disbaled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Other VPN Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>No support</td>
<td>Enabled</td>
</tr>
<tr>
<td>General Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
<td>Opt. lic.: Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>No support</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>716</td>
<td>916</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
<td>2</td>
</tr>
<tr>
<td>Clustering</td>
<td>No Support</td>
<td>2</td>
</tr>
<tr>
<td>IPS Module</td>
<td>Disabled</td>
<td>Optional license: Available</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>50</td>
<td>100</td>
</tr>
</tbody>
</table>

ASA 5515-X

Table 3-3  ASA 5515-X License Features

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
<th>Firewall Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
<td>Optional Time-based license: Available</td>
</tr>
</tbody>
</table>
Table 3-3   ASA 5515-X License Features (continued)

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>250,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>No support</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Disabled</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2</td>
</tr>
</tbody>
</table>

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>250</td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Other VPN Licenses

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>250</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>250</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

General Licenses

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>916</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2</td>
</tr>
<tr>
<td>Clustering</td>
<td>2</td>
</tr>
<tr>
<td>IPS Module</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>100</td>
</tr>
</tbody>
</table>
### ASA 5525-X

**Table 3-4 ASA 5525-X License Features**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>500,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Disabled</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Disabled</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2 Optional licenses: 24 50 100 250 500 750 1000</td>
</tr>
</tbody>
</table>

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.

| AnyConnect Premium Peers (maximum)         | 750                            |
| Adv. Endpoint Assessment                   | Enabled                        |
| AnyConnect for Cisco VPN Phone             | Enabled                        |
| AnyConnect Essentials                      | Disabled                       |
| AnyConnect for Mobile                      | Enabled                        |

**Other VPN Licenses**

| Total VPN Peers, combined all types         | 750                            |
| Other VPN Peers                             | 750                            |
| VPN Load Balancing                          | Enabled                        |

**General Licenses**

| Encryption Base (DES)                      | Optional license: Strong (3DES/AES) |
| Failover Active/Standby or Active/Active   |                               |
| Interfaces of all types, Max.              | 1316                            |
| Security Contexts                          | 2 Optional licenses: 5 10 20     |
| Clustering                                 | 2                               |
| IPS Module                                 | Disabled                        |
| VLANs, Maximum                             | 200                             |

### ASA 5545-X

**Table 3-5 ASA 5545-X License Features**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>750,000</td>
</tr>
</tbody>
</table>
### Table 3-5  ASA 5545-X License Features (continued)

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTP/GPRS</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect Premium Peers</td>
<td>2500</td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Other VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>2500</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>2500</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>1716</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2</td>
</tr>
<tr>
<td>Clustering</td>
<td>2</td>
</tr>
<tr>
<td>IPS Module</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>300</td>
</tr>
</tbody>
</table>

### ASA 5555-X

### Table 3-6  ASA 5555-X License Features

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>1,000,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Disabled</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Disabled</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2 24 50 100 250 500 750 1000 2000 3000</td>
</tr>
</tbody>
</table>
### Supported Feature Licenses Per Model

#### Chapter 3  
**Product Authorization Key Licenses**

**Table 3-6  
ASA 5555-X License Features (continued)**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.</td>
<td></td>
</tr>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>5000</td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Other VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>5000</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>5000</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Encryption                                         | Base (DES)  
Optional license: Strong (3DES/AES)                                      |
| Failover                                           | Active/Standby or Active/Active                                              |
| Interfaces of all types, Max.                       | 2516                                                                         |
| Security Contexts                                  | 2  
Optional licenses:  
5  
10  
20  
50  
100                                                   |
| Clustering                                         | 2                                                                           |
| IPS Module                                         | Disabled  
Optional license: Available                                               |
| VLANs, Maximum                                     | 500                                                                         |

**ASA 5585-X with SSP-10**

You can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-10 with an SSP-20 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.

**Table 3-7  
ASA 5585-X with SSP-10 License Features**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
</tr>
</tbody>
</table>
| Botnet Traffic Filter                              | Disabled  
Optional Time-based license: Available                                     |
| Firewall Conns, Concurrent                         | 1,000,000                                                                    |
| GTP/GPRS                                           | Disabled  
Optional license: Available                                                 |
| Intercompany Media Eng.                            | Disabled  
Optional license: Available                                                 |
| UC Phone Proxy Sessions, Total UC Proxy Sessions    | 2  
Optional licenses:  
24  
50  
100  
250  
500  
750  
1000  
2000  
3000                                               |

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.
### Table 3-7  ASA 5585-X with SSP-10 License Features (continued)

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>5000</td>
</tr>
<tr>
<td></td>
<td><em>Shared licenses: No Support.</em></td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Other VPN Licenses

| Total VPN Peers, combined all types  | 5000                            |
| Other VPN Peers                     | 5000                            |
| VPN Load Balancing                  | Enabled                         |

### General Licenses

| 10 GE I/O Base License               | Disabled; fiber ifcs run at 1 GE |
|                                      | Security Plus License: Enabled; fiber ifcs run at 10 GE |
| Encryption Base (DES)                | *Optional license: Strong (3DES/AES)* |
| Failover Active/Standby or Active/Active |                                  |
| Interfaces of all types, Max.        | 4612                            |
| Security Contexts                    | 2                               |
|                                       | *Optional licenses: 5 10 20 50 100* |
| Clustering                           | Disabled                        |
|                                       | *Optional license: Available for 16 units* |
| VLANs, Maximum                       | 1024                            |

ASA 5585-X with SSP-20

You can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-20 with an SSP-40 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.

### Table 3-8  ASA 5585-X with SSP-20 License Features

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td><em>Optional Time-based license: Available</em></td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>2,000,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td><em>Optional license: Available</em></td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td><em>Optional license: Available</em></td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td><em>Optional licenses: 24 50 100 250 500 750 1000 2000 3000 5000 10,000</em></td>
</tr>
</tbody>
</table>

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.
Table 3-8  **ASA 5585-X with SSP-20 License Features (continued)**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Peers</td>
<td>10,000</td>
</tr>
<tr>
<td>(maximum)</td>
<td></td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Other VPN Licenses**

| Total VPN Peers, combined all types | 10,000 |
| Other VPN Peers                    | 10,000 |
| VPN Load Balancing                 | Enabled |

**General Licenses**

| 10 GE I/O                         | **Base License**: Disabled; fiber ifcs run at 1 GE | **Security Plus License**: Enabled; fiber ifcs run at 10 GE |
| Encryption                        | Base (DES) | Optional license: Strong (3DES/AES) |
| Failover                          | Active/Standby or Active/Active |
| Interfaces of all types, Max.     | 4612 |
| Security Contexts                 | 2 | Optional licenses: 5 10 20 50 100 250 |
| Clustering                        | Disabled | Optional license: Available for 16 units |
| VLANs, Maximum                    | 1024 |

1. With the 10,000-session UC license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.

**ASA 5585-X with SSP-40 and -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.

Table 3-9  **ASA 5585-X with SSP-40 and -60 License Features**

<table>
<thead>
<tr>
<th>Licenses</th>
<th><strong>Base License</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td><strong>5585-X with SSP-40</strong>: 4,000,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Disabled</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Disabled</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2</td>
</tr>
</tbody>
</table>

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.
### Table 3-9  ASA 5585-X with SSP-40 and -60 License Features (continued)

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td><em>Shared licenses: No Support.</em></td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Other VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>10,000</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>10,000</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>10 GE I/O</td>
<td>Enabled; fiber ifcs run at 10 GE</td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>4612</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2</td>
</tr>
<tr>
<td>Clustering</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>1024</td>
</tr>
</tbody>
</table>

1. With the 10,000-session UC license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.

### ASA Services Module

### Table 3-10  ASASM License Features

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>10,000,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Disabled</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Disabled</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>2</td>
</tr>
</tbody>
</table>

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td><em>Shared licenses: No Support.</em></td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Table 3-10  ASASM License Features (continued)

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Other VPN Licenses

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>10,000</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>10,000</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

General Licenses

<table>
<thead>
<tr>
<th>License</th>
<th>Brewery (DES)</th>
<th>Optional license: Strong (3DES/AES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
<td></td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2</td>
<td>Optional licenses:</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>250</td>
</tr>
<tr>
<td>Clustering</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>1000</td>
<td></td>
</tr>
</tbody>
</table>

1. With the 10,000-session UC license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.

ASAv10 (9.3(1))

Table 3-11  ASAv10 License Features

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Supported</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>100,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Supported</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Supported</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>250</td>
</tr>
</tbody>
</table>

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.

<table>
<thead>
<tr>
<th>License</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>250</td>
</tr>
</tbody>
</table>


Adv. Endpoint Assessment                     | Enabled |
AnyConnect for Cisco VPN Phone               | Enabled |
AnyConnect Essentials                         | Disabled|
AnyConnect for Mobile                         | Enabled |
### Table 3-11  **ASA10 License Features (continued)**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other VPN Licenses</td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>250</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>250</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td>General Licenses</td>
<td></td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>1 vCPU</td>
</tr>
<tr>
<td>Encryption</td>
<td>Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>716</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
</tr>
<tr>
<td>Clustering</td>
<td>No support</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>50</td>
</tr>
<tr>
<td>RAM, vCPU Frequency Limit</td>
<td>2 GB, 5000 MHz</td>
</tr>
</tbody>
</table>

### ASA10 (9.3(1))

### Table 3-12  **ASA30 License Features**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Supported</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>500,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Supported</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Supported</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>1000</td>
</tr>
</tbody>
</table>

VPN Licenses require an AnyConnect Plus or Apex license, available separately. See the following maximum values when you purchase an AnyConnect license.

| AnyConnect Premium Peers (maximum) | 750 |
| Shared licenses: No Support. AnyConnect licenses are shared and no longer require a shared server or participant license. |
| Adv. Endpoint Assessment          | Enabled |
| AnyConnect for Cisco VPN Phone    | Enabled |
| AnyConnect Essentials             | Disabled |
| AnyConnect for Mobile             | Enabled |

**Other VPN Licenses**
### Table 3-12  
**ASA v3.0 License Features (continued)**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>750</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>750</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**General Licenses**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Encryption</td>
<td>Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>1316</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
</tr>
<tr>
<td>Clustering</td>
<td>No support</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>200</td>
</tr>
<tr>
<td>RAM, vCPU Frequency Limit</td>
<td>8 GB, 20000 MHz</td>
</tr>
</tbody>
</table>
License Notes

The following table includes additional information about licenses.

<table>
<thead>
<tr>
<th>License</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Essentials</td>
<td>AnyConnect Essentials sessions include the following VPN types: -SSL VPN -IPsec remote access VPN using IKEv2 This license does not support browser-based (clientless) SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium license instead of the AnyConnect Essentials license. <strong>Note</strong> With the AnyConnect Essentials license, VPN users can use a web browser to log in, and download and start (WebLaunch) the AnyConnect client. The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium license. The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given ASA: AnyConnect Premium license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium licenses on different ASAs in the same network. By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the <code>webvpn</code>, and then the <code>no anyconnect-essentials</code> command or in ASDM, using the Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; AnyConnect Essentials pane.</td>
</tr>
</tbody>
</table>
## Table 3-13 License Notes (continued)

<table>
<thead>
<tr>
<th>License</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect for Mobile</td>
<td>This license provides access to the AnyConnect Client for touch-screen mobile devices running Windows Mobile 5.0, 6.0, and 6.1. We recommend using this license if you want to support mobile access to AnyConnect 2.3 and later versions. This license requires activation of one of the following licenses to specify the total number of SSL VPN sessions permitted: AnyConnect Essentials or AnyConnect Premium.</td>
</tr>
<tr>
<td></td>
<td><strong>Mobile Posture Support</strong></td>
</tr>
<tr>
<td></td>
<td>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. Here is the functionality you receive based on the license you install.</td>
</tr>
<tr>
<td></td>
<td>• AnyConnect Premium License Functionality</td>
</tr>
<tr>
<td></td>
<td>– Enforce DAP policies on supported mobile devices based on DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device.</td>
</tr>
<tr>
<td></td>
<td>• AnyConnect Essentials License Functionality</td>
</tr>
<tr>
<td></td>
<td>– Enable or disable mobile device access on a per group basis and to configure that feature using ASDM.</td>
</tr>
<tr>
<td></td>
<td>– 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.</td>
</tr>
<tr>
<td>AnyConnect Premium</td>
<td>AnyConnect Premium sessions include the following VPN types:</td>
</tr>
<tr>
<td></td>
<td>• SSL VPN</td>
</tr>
<tr>
<td></td>
<td>• Clientless SSL VPN</td>
</tr>
<tr>
<td></td>
<td>• IPsec remote access VPN using IKEv2</td>
</tr>
<tr>
<td>AnyConnect Premium</td>
<td>A shared license lets the ASA act as a shared license server for multiple client ASAs. The shared license pool is large, but the maximum number of sessions used by each individual ASA cannot exceed the maximum number listed for permanent licenses.</td>
</tr>
<tr>
<td>Shared</td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Requires a Strong Encryption (3DES/AES) License to download the dynamic database.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The DES license cannot be disabled. If you have the 3DES license installed, DES is still available. To prevent the use of DES when you want to only use strong encryption, be sure to configure any relevant commands to use only strong encryption.</td>
</tr>
</tbody>
</table>
When you enable the Intercompany Media Engine (IME) license, you can use TLS proxy sessions up to the configured TLS proxy limit. If you also have a Unified Communications (UC) license installed that is higher than the default TLS proxy limit, then the ASA sets the limit to be the UC license limit plus an additional number of sessions depending on your model. You can manually configure the TLS proxy limit using the `tls-proxy maximum-sessions` command or in ASDM, using the `Configuration > Firewall > Unified Communications > TLS Proxy` pane. To view the limits of your model, enter the `tls-proxy maximum-sessions ?` command. If you also install the UC license, then the TLS proxy sessions available for UC are also available for IME sessions. For example, if the configured limit is 1000 TLS proxy sessions, and you purchase a 750-session UC license, then the first 250 IME sessions do not affect the sessions available for UC. If you need more than 250 sessions for IME, then the remaining 750 sessions of the platform limit are used on a first-come, first-served basis by UC and IME.

- For a license part number ending in “K8”, TLS proxy sessions are limited to 1000.
- For a license part number ending in “K9”, the TLS proxy limit depends on your configuration and the platform model.

**Note** K8 and K9 refer to whether the license is restricted for export: K8 is unrestricted, and K9 is restricted.

You might also use SRTP encryption sessions for your connections:

- For a K8 license, SRTP sessions are limited to 250.
- For a K9 license, there is no limit.

**Note** Only calls that require encryption/decryption for media are counted toward the SRTP limit; if passthrough is set for the call, even if both legs are SRTP, they do not count toward the limit.

The maximum number of combined interfaces; for example, VLANs, physical, redundant, bridge group, and EtherChannel interfaces. Every `interface` command defined in the configuration counts against this limit. For example, both of the following interfaces count even if the GigabitEthernet 0/0 interface is defined as part of port-channel 1:

```
interface gigabitethernet 0/0
```

and

```
interface port-channel 1
```
The IPS module license lets you run the IPS software module on the ASA. You also need the IPS signature subscription on the IPS side.

See the following guidelines:

- To buy the IPS signature subscription you need to have the ASA with IPS pre-installed (the part number must include “IPS”, for example ASA5515-IPS-K9); you cannot buy the IPS signature subscription for a non-IPS part number ASA.

- For failover, you need the IPS signature subscription on both units; this subscription is not shared in failover, because it is not an ASA license.

- For failover, the IPS signature subscription requires a unique IPS module license per unit. Like other ASA licenses, the IPS module license is technically shared in the failover cluster license. However, because of the IPS signature subscription requirements, you must buy a separate IPS module license for each unit in failover.

Other VPN sessions include the following VPN types:

- IPsec remote access VPN using IKEv1
- IPsec site-to-site VPN using IKEv1
- IPsec site-to-site VPN using IKEv2

This license is included in the Base license.

Although the maximum VPN sessions add up to more than the maximum VPN AnyConnect and Other VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the ASA, so be sure to size your network appropriately.

If you start a clientless SSL VPN session and then start an AnyConnect client session from the portal, 1 session is used in total. However, if you start the AnyConnect client first (from a standalone client, for example) and then log into the clientless SSL VPN portal, then 2 sessions are used.

<table>
<thead>
<tr>
<th>License</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS module</td>
<td>The IPS module license lets you run the IPS software module on the ASA. You also need the IPS signature subscription on the IPS side.</td>
</tr>
<tr>
<td></td>
<td>See the following guidelines:</td>
</tr>
<tr>
<td></td>
<td>- To buy the IPS signature subscription you need to have the ASA with IPS pre-installed (the part number must include “IPS”, for example ASA5515-IPS-K9); you cannot buy the IPS signature subscription for a non-IPS part number ASA.</td>
</tr>
<tr>
<td></td>
<td>- For failover, you need the IPS signature subscription on both units; this subscription is not shared in failover, because it is not an ASA license.</td>
</tr>
<tr>
<td></td>
<td>- For failover, the IPS signature subscription requires a unique IPS module license per unit. Like other ASA licenses, the IPS module license is technically shared in the failover cluster license. However, because of the IPS signature subscription requirements, you must buy a separate IPS module license for each unit in failover.</td>
</tr>
<tr>
<td>Other VPN</td>
<td>Other VPN sessions include the following VPN types:</td>
</tr>
<tr>
<td></td>
<td>- IPsec remote access VPN using IKEv1</td>
</tr>
<tr>
<td></td>
<td>- IPsec site-to-site VPN using IKEv1</td>
</tr>
<tr>
<td></td>
<td>- IPsec site-to-site VPN using IKEv2</td>
</tr>
<tr>
<td></td>
<td>This license is included in the Base license.</td>
</tr>
<tr>
<td>Total VPN (sessions), combined all types</td>
<td>- Although the maximum VPN sessions add up to more than the maximum VPN AnyConnect and Other VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the ASA, so be sure to size your network appropriately.</td>
</tr>
<tr>
<td></td>
<td>- If you start a clientless SSL VPN session and then start an AnyConnect client session from the portal, 1 session is used in total. However, if you start the AnyConnect client first (from a standalone client, for example) and then log into the clientless SSL VPN portal, then 2 sessions are used.</td>
</tr>
</tbody>
</table>
The following applications use TLS proxy sessions for their connections. Each TLS proxy session used by these applications (and only these applications) is counted against the UC license limit:

- Phone Proxy
- Presence Federation Proxy
- Encrypted Voice Inspection

Other applications that use TLS proxy sessions do not count toward the UC limit, for example, Mobility Advantage Proxy (which does not require a license) and IME (which requires a separate IME license).

Some UC applications might use multiple sessions for a connection. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS proxy connections, so 2 UC Proxy sessions are used.

You independently set the TLS proxy limit using the `tls-proxy maximum-sessions` command or in ASDM, using the Configuration > Firewall > Unified Communications > TLS Proxy pane.

To view the limits of your model, enter the `tls-proxy maximum-sessions ?` command. When you apply a UC license that is higher than the default TLS proxy limit, the ASA automatically sets the TLS proxy limit to match the UC limit. The TLS proxy limit takes precedence over the UC license limit; if you set the TLS proxy limit to be less than the UC license, then you cannot use all of the sessions in your UC license.

**Note**

For license part numbers ending in “K8” (for example, licenses under 250 users), TLS proxy sessions are limited to 1000. For license part numbers ending in “K9” (for example, licenses 250 users or larger), the TLS proxy limit depends on the configuration, up to the model limit. K8 and K9 refer to whether the license is restricted for export: K8 is unrestricted, and K9 is restricted.

If you clear the configuration (using the `clear configure all` command, for example), then the TLS proxy limit is set to the default for your model; if this default is lower than the UC license limit, then you see an error message to use the `tls-proxy maximum-sessions` command to raise the limit again (in ASDM, use the TLS Proxy pane). If you use failover and enter the `write standby` command or in ASDM, use File > Save Running Configuration to Standby Unit on the primary unit to force a configuration synchronization, the `clear configure all` command is generated on the secondary unit automatically, so you may see the warning message on the secondary unit. Because the configuration synchronization restores the TLS proxy limit set on the primary unit, you can ignore the warning.

You might also use SRTP encryption sessions for your connections:

- For K8 licenses, SRTP sessions are limited to 250.
- For K9 licenses, there is no limit.

**Note**

Only calls that require encryption/decryption for media are counted toward the SRTP limit; if passthrough is set for the call, even if both legs are SRTP, they do not count toward the limit.

### Virtual CPU

You must install a model license on the ASAv that sets the appropriate number of vCPUs. Until you install a license, throughput is limited to 100 Kbps so that you can perform preliminary connectivity tests. A model license is required for regular operation.
Table 3-13  License Notes (continued)

<table>
<thead>
<tr>
<th>License</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANs, Maximum</td>
<td>For an interface to count against the VLAN limit, you must assign a VLAN to it. For example:</td>
</tr>
<tr>
<td></td>
<td>\texttt{interface gigabitethernet 0/0.100}</td>
</tr>
<tr>
<td></td>
<td>\texttt{vlan 100}</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>VPN load balancing requires a Strong Encryption (3DES/AES) License.</td>
</tr>
</tbody>
</table>

About PAK Licenses

A license specifies the options that are enabled on a given ASA. It is represented by an activation key that is a 160-bit (5 32-bit words or 20 bytes) value. This value encodes the serial number (an 11 character string) and the enabled features.

- Preinstalled License, page 3-20
- Permanent License, page 3-20
- Time-Based Licenses, page 3-21
- Shared AnyConnect Premium Licenses, page 3-23
- Failover or ASA Cluster Licenses, page 3-23
- No Payload Encryption Models, page 3-27
- Licenses FAQ, page 3-27

Preinstalled License

By default, your ASA ships with a license already installed. This license might be the Base License, to which you want to add more licenses, or it might already have all of your licenses installed, depending on what you ordered and what your vendor installed for you.

Related Topics
Monitoring PAK Licenses, page 3-38

Permanent License

You can have one permanent activation key installed. The permanent activation key includes all licensed features in a single key. If you also install time-based licenses, the ASA combines the permanent and time-based licenses into a running license.

Related Topics
How Permanent and Time-Based Licenses Combine, page 3-21
Time-Based Licenses

In addition to permanent licenses, you can purchase time-based licenses or receive an evaluation license that has a time-limit. For example, you might buy a time-based AnyConnect Premium license to handle short-term surges in the number of concurrent SSL VPN users, or you might order a Botnet Traffic Filter time-based license that is valid for 1 year.

- Time-Based License Activation Guidelines, page 3-21
- How the Time-Based License Timer Works, page 3-21
- How Permanent and Time-Based Licenses Combine, page 3-21
- Stacking Time-Based Licenses, page 3-22
- Time-Based License Expiration, page 3-23

Time-Based License Activation Guidelines

- You can install multiple time-based licenses, including multiple licenses for the same feature. However, only one time-based license per feature can be active at a time. The inactive license remains installed, and ready for use. For example, if you install a 1000-session AnyConnect Premium license, and a 2500-session AnyConnect Premium license, then only one of these licenses can be active.
- If you activate an evaluation license that has multiple features in the key, then you cannot also activate another time-based license for one of the included features. For example, if an evaluation license includes the Botnet Traffic Filter and a 1000-session AnyConnect Premium license, you cannot also activate a standalone time-based 2500-session AnyConnect Premium license.

How the Time-Based License Timer Works

- The timer for the time-based license starts counting down when you activate it on the ASA.
- If you stop using the time-based license before it times out, then the timer halts. The timer only starts again when you reactivate the time-based license.
- If the time-based license is active, and you shut down the ASA, then the timer continues to count down. If you intend to leave the ASA in a shut down state for an extended period of time, then you should deactivate the time-based license before you shut down.

Note

We suggest you do not change the system clock after you install the time-based license. If you set the clock to be a later date, then if you reload, the ASA checks the system clock against the original installation time, and assumes that more time has passed than has actually been used. If you set the clock back, and the actual running time is greater than the time between the original installation time and the system clock, then the license immediately expires after a reload.

How Permanent and Time-Based Licenses Combine

When you activate a time-based license, then features from both permanent and time-based licenses combine to form the running license. How the permanent and time-based licenses combine depends on the type of license. The following table lists the combination rules for each feature license.
About PAK Licenses

Note

Even when the permanent license is used, if the time-based license is active, it continues to count down.

Related Topics
Monitoring PAK Licenses, page 3-38

Stacking Time-Based Licenses

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 stack time-based licenses so that you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early.

When you install an identical time-based license as one already installed, then the licenses are combined, and the duration equals the combined duration.

For example:

1. You install a 52-week Botnet Traffic Filter license, and use the license for 25 weeks (27 weeks remain).
2. You then purchase another 52-week Botnet Traffic Filter license. When you install the second license, the licenses combine to have a duration of 79 weeks (52 weeks plus 27 weeks).

Table 3-14  Time-Based License Combination Rules

<table>
<thead>
<tr>
<th>Time-Based Feature</th>
<th>Combined License Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium</td>
<td>The higher value is used, either time-based or permanent. For example, if the permanent license is 1000 sessions, and the time-based license is</td>
</tr>
<tr>
<td>Sessions</td>
<td>2500 sessions, then 2500 sessions are enabled. Typically, you will not install a time-based license that has less capability than the permanent</td>
</tr>
<tr>
<td></td>
<td>license, but if you do so, then the permanent license is used.</td>
</tr>
<tr>
<td>Unified Communications</td>
<td>The time-based license sessions are added to the permanent sessions, up to the platform limit. For example, if the permanent license is 2500</td>
</tr>
<tr>
<td>Proxy Sessions</td>
<td>sessions, and the time-based license is 1000 sessions, then 3500 sessions are enabled for as long as the time-based license is active.</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>The time-based license contexts are added to the permanent contexts, up to the platform limit. For example, if the permanent license is 10</td>
</tr>
<tr>
<td></td>
<td>contexts, and the time-based license is 20 contexts, then 30 contexts are enabled for as long as the time-based license is active.</td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>There is no permanent Botnet Traffic Filter license available; the time-based license is used.</td>
</tr>
<tr>
<td>All Others</td>
<td>The higher value is used, either time-based or permanent. For licenses that have a status of enabled or disabled, then the license with the</td>
</tr>
<tr>
<td></td>
<td>enabled status is used. For licenses with numerical tiers, the higher value is used. Typically, you will not install a time-based license that</td>
</tr>
<tr>
<td></td>
<td>has less capability than the permanent license, but if you do so, then the permanent license is used.</td>
</tr>
</tbody>
</table>
Similarly:

1. You install an 8-week 1000-session AnyConnect Premium license, and use it for 2 weeks (6 weeks remain).
2. You then install another 8-week 1000-session license, and the licenses combine to be 1000-sessions for 14 weeks (8 weeks plus 6 weeks).

If the licenses are not identical (for example, a 1000-session AnyConnect Premium license vs. a 2500-session license), then the licenses are not combined. Because only one time-based license per feature can be active, only one of the licenses can be active.

Although non-identical licenses do not combine, when the current license expires, the ASA automatically activates an installed license of the same feature if available.

Related Topics
- Activate or Deactivate Keys, page 3-30
- Time-Based License Expiration, page 3-23

Time-Based License Expiration

When the current license for a feature expires, the ASA automatically activates an installed license of the same feature if available. If there are no other time-based licenses available for the feature, then the permanent license is used.

If you have more than one additional time-based license installed for a feature, then the ASA uses the first license it finds; which license is used is not user-configurable and depends on internal operations. If you prefer to use a different time-based license than the one the ASA activated, then you must manually activate the license you prefer.

For example, you have a time-based 2500-session AnyConnect Premium license (active), a time-based 1000-session AnyConnect Premium license (inactive), and a permanent 500-session AnyConnect Premium license. While the 2500-session license expires, the ASA activates the 1000-session license. After the 1000-session license expires, the ASA uses the 500-session permanent license.

Related Topics
Activate or Deactivate Keys, page 3-30

Shared AnyConnect Premium Licenses

Note
The shared license feature on the ASA is not supported with newer AnyConnect licensing.

A shared license lets you purchase a large number of AnyConnect Premium sessions and share the sessions as needed among a group of ASAs by configuring one of the ASAs as a shared licensing server, and the rest as shared licensing participants.

Failover or ASA Cluster Licenses

With some exceptions, failover and cluster units do not require the same license on each unit. For earlier versions, see the licensing document for your version.
Failover License Requirements and Exceptions

Failover units do not require the same license on each unit. Typically, you buy a license only for the primary unit; for Active/Standby failover, the secondary unit inherits the primary license when it becomes active. If you have licenses on both units, they combine into a single running failover cluster license. There are some exceptions to this rule. See the following table for precise licensing requirements for failover.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>• Active/Standby—Security Plus License.</td>
</tr>
<tr>
<td></td>
<td>• Active/Active—No Support.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>ASA 5512-X through ASA 5555-X</td>
<td>• ASA 5512-X—Security Plus License.</td>
</tr>
<tr>
<td></td>
<td>• Other models—Base License.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Each unit must have the same encryption license; each unit must have the same IPS module license. You also need the IPS signature subscription on the IPS side for both units. See the following guidelines:</td>
</tr>
<tr>
<td></td>
<td>- To buy the IPS signature subscription you need to have the ASA with IPS pre-installed (the part number must include “IPS”, for example ASA5515-IPS-K9); you cannot buy the IPS signature subscription for a non-IPS part number ASA.</td>
</tr>
<tr>
<td></td>
<td>- You need the IPS signature subscription on both units; this subscription is not shared in failover, because it is not an ASA license.</td>
</tr>
<tr>
<td></td>
<td>- The IPS signature subscription requires a unique IPS module license per unit. Like other ASA licenses, the IPS module license is technically shared in the failover cluster license. However, because of the IPS signature subscription requirements, you must buy a separate IPS module license for each unit in.</td>
</tr>
<tr>
<td>ASAv</td>
<td>• Active/Standby—Standard and Premium Licenses.</td>
</tr>
<tr>
<td></td>
<td>• Active/Active—No Support.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The standby unit requires the same model license as the primary unit; Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>All other models</td>
<td>Base License.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Each unit must have the same encryption license.</td>
</tr>
</tbody>
</table>
About PAK Licenses

Note
A valid permanent key is required; in rare instances, your authentication key can be removed. If your key consists of all 0’s, then you need to reinstall a valid authentication key before failover can be enabled.

ASA Cluster License Requirements and Exceptions

Cluster units do not require the same license on each unit. Typically, you buy a license only for the master unit; slave units inherit the master license. If you have licenses on multiple units, they combine into a single running ASA cluster license.

There are exceptions to this rule. See the following table for precise licensing requirements for clustering.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5585-X</td>
<td>Cluster License.</td>
</tr>
<tr>
<td>Note</td>
<td>Each unit must have the same encryption license; each unit must have the same 10 GE I/O/Security Plus license (ASA 5585-X with SSP-10 and -20).</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>Security Plus license.</td>
</tr>
<tr>
<td>Note</td>
<td>Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>Note</td>
<td>Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>All other models</td>
<td>No support.</td>
</tr>
</tbody>
</table>

How Failover or ASA Cluster Licenses Combine

For failover pairs or ASA clusters, the licenses on each unit are combined into a single running cluster license. If you buy separate licenses for each unit, then the combined license uses the following rules:

- For licenses that have numerical tiers, such as the number of sessions, the values from each unit’s licenses are combined up to the platform limit. If all licenses in use are time-based, then the licenses count down simultaneously.

  For example, for failover:
  - You have two ASAs with 10 AnyConnect Premium sessions installed on each; the licenses will be combined for a total of 20 AnyConnect Premium sessions.
  - You have two ASA 5525-Xs with 500 AnyConnect Premium sessions each; because the platform limit is 750, the combined license allows 750 AnyConnect Premium sessions.

Note
In the above example, if the AnyConnect Premium licenses are time-based, you might want to disable one of the licenses so that you do not “waste” a 500 session license from which you can only use 250 sessions because of the platform limit.
About PAK Licenses

- You have two ASA 5545-X ASAs, one with 20 contexts and the other with 10 contexts; the combined license allows 30 contexts. For Active/Active failover, the contexts are divided between the two units. One unit can use 18 contexts and the other unit can use 12 contexts, for example, for a total of 30.

For example, for ASA clustering:

- You have four ASA 5585-X ASAs with SSP-10, three units with 50 contexts each, and one unit with the default 2 contexts. Because the platform limit is 100, the combined license allows a maximum of 100 contexts. Therefore, you can configure up to 100 contexts on the master unit; each slave unit will also have 100 contexts through configuration replication.

- You have four ASA 5585-X ASAs with SSP-60, three units with 50 contexts each, and one unit with the default 2 contexts. Because the platform limit is 250, the licenses will be combined for a total of 152 contexts. Therefore, you can configure up to 152 contexts on the master unit; each slave unit will also have 152 contexts through configuration replication.

- For licenses that have a status of enabled or disabled, then the license with the enabled status is used.

- For time-based licenses that are enabled or disabled (and do not have numerical tiers), the duration is the combined duration of all licenses. The primary/master unit counts down its license first, and when it expires, the secondary/slave unit(s) start counting down its license, and so on. This rule also applies to Active/Active failover and ASA clustering, even though all units are actively operating.

For example, if you have 48 weeks left on the Botnet Traffic Filter license on two units, then the combined duration is 96 weeks.

Related Topics

Monitoring PAK Licenses, page 3-38

Loss of Communication Between Failover or ASA Cluster Units

If the units lose communication for more than 30 days, then each unit reverts to the license installed locally. During the 30-day grace period, the combined running license continues to be used by all units.

If you restore communication during the 30-day grace period, then for time-based licenses, the time elapsed is subtracted from the primary/master license; if the primary/master license becomes expired, only then does the secondary/slave license start to count down.

If you do not restore communication during the 30-day period, then for time-based licenses, time is subtracted from all unit licenses, if installed. They are treated as separate licenses and do not benefit from the combined license. The time elapsed includes the 30-day grace period.

For example:

1. You have a 52-week Botnet Traffic Filter license installed on two units. The combined running license allows a total duration of 104 weeks.

2. The units operate as a failover unit/ASA cluster for 10 weeks, leaving 94 weeks on the combined license (42 weeks on the primary/master, and 52 weeks on the secondary/slave).

3. If the units lose communication (for example the primary/master unit fails), the secondary/slave unit continues to use the combined license, and continues to count down from 94 weeks.

4. The time-based license behavior depends on when communication is restored:

   - Within 30 days—The time elapsed is subtracted from the primary/master unit license. In this case, communication is restored after 4 weeks. Therefore, 4 weeks are subtracted from the primary/master license leaving 90 weeks combined (38 weeks on the primary, and 52 weeks on the secondary).
About PAK Licenses

After 30 days—The time elapsed is subtracted from both units. In this case, communication is restored after 6 weeks. Therefore, 6 weeks are subtracted from both the primary/master and secondary/slave licenses, leaving 84 weeks combined (36 weeks on the primary/master, and 46 weeks on the secondary/slave).

Upgrading Failover Pairs

Because failover pairs do not require the same license on both units, you can apply new licenses to each unit without any downtime. If you apply a permanent license that requires a reload, then you can fail over to the other unit while you reload. If both units require reloading, then you can reload them separately so that you have no downtime.

Related Topics
Table 3-15 on page 3-30

No Payload Encryption Models

You can purchase some models with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA series. The ASA software senses a No Payload Encryption model, and disables the following features:

- Unified Communications
- VPN

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 Filter (which uses SSL).

When you view the license, VPN and Unified Communications licenses will not be listed.

Related Topics
Monitoring PAK Licenses, page 3-38

Licenses FAQ

Q. Can I activate multiple time-based licenses, for example, AnyConnect Premium and Botnet Traffic Filter?
A. Yes. You can use one time-based license per feature at a time.

Q. Can I “stack” time-based licenses so that when the time limit runs out, it will automatically use the next license?
A. Yes. For identical licenses, the time limit is combined when you install multiple time-based licenses. For non-identical licenses (for example, a 1000-session AnyConnect Premium license and a 2500-session license), the ASA automatically activates the next time-based license it finds for the feature.

Q. Can I install a new permanent license while maintaining an active time-based license?
A. Yes. Activating a permanent license does not affect time-based licenses.
Q. For failover, can I use a shared licensing server as the primary unit, and the shared licensing backup server as the secondary unit?

A. No. The secondary unit has the same running license as the primary unit; in the case of the shared licensing server, they require a server license. The backup server requires a participant license. The backup server can be in a separate failover pair of two backup servers.

Q. Do I need to buy the same licenses for the secondary unit in a failover pair?

A. No. Starting with Version 8.3(1), you do not have to have matching licenses on both units. Typically, you buy a license only for the primary unit; the secondary unit inherits the primary license when it becomes active. In the case where you also have a separate license on the secondary unit (for example, if you purchased matching licenses for pre-8.3 software), the licenses are combined into a running failover cluster license, up to the model limits.

Q. Can I use a time-based or permanent AnyConnect Premium license in addition to a shared AnyConnect Premium license?

A. Yes. The shared license is used only after the sessions from the locally installed license (time-based or permanent) are used up. Note: On the shared licensing server, the permanent AnyConnect Premium license is not used; you can however use a time-based license at the same time as the shared licensing server license. In this case, the time-based license sessions are available for local AnyConnect Premium sessions only; they cannot be added to the shared licensing pool for use by participants.

Guidelines for PAK Licenses

Context Mode Guidelines

In multiple context mode, apply the activation key in the system execution space.

Failover Guidelines

See Failover or ASA Cluster Licenses, page 3-23.

Model Guidelines

• Smart Software Licensing is supported on the ASAv only.
• Shared licenses are not supported on the ASAv or ASA 5506-X.

Upgrade and Downgrade Guidelines

Your activation key remains compatible if you upgrade to the latest version from any previous version. However, you might have issues if you want to maintain downgrade capability:

• Downgrading to Version 8.1 or earlier—After you upgrade, if you activate additional feature licenses that were introduced before 8.2, then the activation key continues to be compatible with earlier versions if you downgrade. However if you activate feature licenses that were introduced in 8.2 or later, then the activation key is not backwards compatible. If you have an incompatible license key, then see the following guidelines:
  – If you previously entered an activation key in an earlier version, then the ASA uses that key (without any of the new licenses you activated in Version 8.2 or later).
  – If you have a new system and do not have an earlier activation key, then you need to request a new activation key compatible with the earlier version.
Configure PAK Licenses

This section describes how to obtain an activation key and how to active it. You can also deactivate a key.

- Obtain an Activation Key, page 3-30
- Activate or Deactivate Keys, page 3-30
Obtain an Activation Key

To obtain an activation key, you need a Product Authorization Key, which you can purchase from your Cisco account representative. You need to purchase a separate Product Authorization Key for each feature license. For example, if you have the Base License, you can purchase separate keys for Advanced Endpoint Assessment and for additional AnyConnect Premium sessions.

After obtaining the Product Authorization Keys, register them on Cisco.com by performing the following steps.

**Procedure**

**Step 1**
Obtain the serial number for your ASA by entering the following command.

```
ciscoasa# show version | grep Serial
```

**Step 2**
If you are not already registered with Cisco.com, create an account.

**Step 3**
Go to the following licensing website:

```
http://www.cisco.com/go/license
```

**Step 4**
Enter the following information, when prompted:

- Product Authorization Key (if you have multiple keys, enter one of the keys first. You have to enter each key as a separate process.)
- The serial number of your ASA
- Your e-mail address

An activation key is automatically generated and sent to the e-mail address that you provide. This key includes all features you have registered so far for permanent licenses. For time-based licenses, each license has a separate activation key.

**Step 5**
If you have additional Product Authorization Keys, repeat Step 4 for each Product Authorization Key. After you enter all of the Product Authorization Keys, the final activation key provided includes all of the permanent features you registered.

Activate or Deactivate Keys

This section describes how to enter a new activation key, and how to activate and deactivate time-based keys.

**Before You Begin**

- If you are already in multiple context mode, enter the activation key in the system execution space.
- Some permanent licenses require you to reload the ASA after you activate them. The following table lists the licenses that require reloading.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Action Requiring Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>All models</td>
<td>Downgrading the Encryption license.</td>
</tr>
<tr>
<td>ASAv</td>
<td>Downgrading the vCPU license.</td>
</tr>
</tbody>
</table>
## Configure a Shared License

### Procedure

#### Step 1
Apply an activation key to the ASA:

```
activation-key  key  [activate | deactivate]
```

Example:

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

The *key* is a five-element hexadecimal string with one space between each element. The leading 0x specifier is optional; all values are assumed to be hexadecimal.

You can install one permanent key, and multiple time-based keys. If you enter a new permanent key, it overwrites the already installed one.

The *activate* and *deactivate* keywords are available for time-based keys only. If you do not enter any value, *activate* is the default. The last time-based key that you activate for a given feature is the active one. To deactivate any active time-based key, enter the *deactivate* keyword. If you enter a key for the first time, and specify *deactivate*, then the key is installed on the ASA in an inactive state.

#### Step 2
(Might be required.) Reload the ASA:

```
reload
```

Some permanent licenses require you to reload the ASA after entering the new activation key. If you need to reload, you will see the following message:

```
WARNING: The running activation key was not updated with the requested key. The flash activation key was updated with the requested key, and will become active after the next reload.
```

### Related Topics

- Time-Based Licenses, page 3-21
- Table 3-15 on page 3-30

### Configure a Shared License

#### Note
The shared license feature on the ASA is not supported with newer AnyConnect licensing.

This section describes how to configure the shared licensing server and participants.

- About Shared Licenses, page 3-32
- Configure the Shared Licensing Server, page 3-36
- Configure the Shared Licensing Backup Server (Optional), page 3-37
- Configure the Shared Licensing Participant, page 3-38
About Shared Licenses

A shared license lets you purchase a large number of AnyConnect Premium sessions and share the sessions as needed among a group of ASAs by configuring one of the ASAs as a shared licensing server, and the rest as shared licensing participants.

- About the Shared Licensing Server and Participants, page 3-32
- Communication Issues Between Participant and Server, page 3-33
- About the Shared Licensing Backup Server, page 3-33
- Failover and Shared Licenses, page 3-34
- Maximum Number of Participants, page 3-35

About the Shared Licensing Server and Participants

The following steps describe how shared licenses operate:

1. Decide which ASA should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which ASAs should be shared licensing participants, including the shared licensing backup server, and obtain a shared licensing participant license for each device, using each device serial number.
3. (Optional) Designate a second ASA as a shared licensing backup server. You can only specify one backup server.

   Note: The shared licensing backup server only needs a participant license.

4. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
5. When you configure the ASA as a participant, it registers with the shared licensing server by sending information about itself, including the local license and model information.

   Note: The participant needs to be able to communicate with the server over the IP network; it does not have to be on the same subnet.

6. The shared licensing server responds with information about how often the participant should poll the server.
7. When a participant uses up the sessions of the local license, it sends a request to the shared licensing server for additional sessions in 50-session increments.
8. The shared licensing server responds with a shared license. The total sessions used by a participant cannot exceed the maximum sessions for the platform model.

   Note: The shared licensing server can also participate in the shared license pool. It does not need a participant license as well as the server license to participate.

   a. If there are not enough sessions left in the shared license pool for the participant, then the server responds with as many sessions as available.
b. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.

9. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

**Note**
The ASA uses SSL between the server and participant to encrypt all communications.

**Communication Issues Between Participant and Server**

See the following guidelines for communication issues between the participant and server:

- If a participant fails to send a refresh after 3 times the refresh interval, then the server releases the sessions back into the shared license pool.
- If the participant cannot reach the license server to send the refresh, then the participant can continue to use the shared license it received from the server for up to 24 hours.
- If the participant is still not able to communicate with a license server after 24 hours, then the participant releases the shared license, even if it still needs the sessions. The participant leaves existing connections established, but cannot accept new connections beyond the license limit.
- If a participant reconnects with the server before 24 hours expires, but after the server expired the participant sessions, then the participant needs to send a new request for the sessions; the server responds with as many sessions as can be reassigned to that participant.

**About the Shared Licensing Backup Server**

The shared licensing backup server must register successfully with the main shared licensing server before it can take on the backup role. When it registers, the main shared licensing server syncs server settings as well as the shared license information with the backup, including a list of registered participants and the current license usage. The main server and backup server sync the data at 10 second intervals. After the initial sync, the backup server can successfully perform backup duties, even after a reload.

When the main server goes down, the backup server takes over server operation. The backup server can operate for up to 30 continuous days, after which the backup server stops issuing sessions to participants, and existing sessions time out. Be sure to reinstate the main server within that 30-day period. Critical-level syslog messages are sent at 15 days, and again at 30 days.

When the main server comes back up, it syncs with the backup server, and then takes over server operation.

When the backup server is not active, it acts as a regular participant of the main shared licensing server.

**Note**
When you first launch the main shared licensing server, the backup server can only operate independently for 5 days. The operational limit increases day-by-day, until 30 days is reached. Also, if the main server later goes down for any length of time, the backup server operational limit decrements day-by-day. When the main server comes back up, the backup server starts to increment again day-by-day. For example, if the main server is down for 20 days, with the backup server active during that time, then the backup server will only have a 10-day limit left over. The backup server “recharges” up to the maximum 30 days after 20 more days as an inactive backup. This recharging function is implemented to discourage misuse of the shared license.
Failover and Shared Licenses

This section describes how shared licenses interact with failover.

- Failover and Shared License Servers, page 3-34
- Failover and Shared License Participants, page 3-35

Failover and Shared License Servers

This section describes how the main server and backup server interact with failover. Because the shared licensing server is also performing normal duties as the ASA, including performing functions such as being a VPN gateway and firewall, then you might need to configure failover for the main and backup shared licensing servers for increased reliability.

Note

The backup server mechanism is separate from, but compatible with, failover.

Shared licenses are supported only in single context mode, so Active/Active failover is not supported.

For Active/Standby failover, the primary unit acts as the main shared licensing server, and the standby unit acts as the main shared licensing server after failover. The standby unit does not act as the backup shared licensing server. Instead, you can have a second pair of units acting as the backup server, if desired.

For example, you have a network with 2 failover pairs. Pair #1 includes the main licensing server. Pair #2 includes the backup server. When the primary unit from Pair #1 goes down, the standby unit immediately becomes the new main licensing server. The backup server from Pair #2 never gets used. Only if both units in Pair #1 go down does the backup server in Pair #2 come into use as the shared licensing server. If Pair #1 remains down, and the primary unit in Pair #2 goes down, then the standby unit in Pair #2 comes into use as the shared licensing server (see Figure 3-1).
Chapter 3  Product Authorization Key Licenses

Configure a Shared License

Figure 3-1  Failover and Shared License Servers

Key
Blue=Shared license server in use
(Active)=Active failover unit

1. Normal operation:

Failover Pair #1
Main (Active)  Main (Standby)

Failover Pair #2
Backup (Active)  Backup (Standby)

2. Primary main server fails over:

Failover Pair #1
Main (Failed)  Main (Active)

Failover Pair #2
Backup (Active)  Backup (Standby)

3. Both main servers fail:

Failover Pair #1
Main (Failed)  Main (Failed)

Failover Pair #2
Backup (Active)  Backup (Standby)

4. Both main servers and primary backup fail:

Failover Pair #1
Main (Failed)  Main (Failed)

Failover Pair #2
Backup (Failed)  Backup (Active)

The standby backup server shares the same operating limits as the primary backup server; if the standby unit becomes active, it continues counting down where the primary unit left off.

Related Topics
About the Shared Licensing Backup Server, page 3-33

Failover and Shared License Participants

For participant pairs, both units register with the shared licensing server using separate participant IDs. The active unit syncs its participant ID with the standby unit. The standby unit uses this ID to generate a transfer request when it switches to the active role. This transfer request is used to move the shared sessions from the previously active unit to the new active unit.

Maximum Number of Participants

The ASA does not limit the number of participants for the shared license; however, a very large shared network could potentially affect the performance on the licensing server. In this case, you can increase the delay between participant refreshes, or you can create two shared networks.
Configure the Shared Licensing Server

This section describes how to configure the ASA to be a shared licensing server.

**Before You Begin**

The server must have a shared licensing server key.

**Procedure**

**Step 1**
Set the shared secret:

```
license-server secret secret
```

Example:
```
ciscoasa(config)# license-server secret farscape
```

The *secret* is a string between 4 and 128 ASCII characters. Any participant with this secret can use the licensing server.

**Step 2** (Optional) Set the refresh interval:

```
license-server refresh-interval seconds
```

Example:
```
ciscoasa(config)# license-server refresh-interval 100
```

The interval is between 10 and 300 seconds; this value is provided to participants to set how often they should communicate with the server. The default is 30 seconds.

**Step 3** (Optional) Set the port on which the server listens for SSL connections from participants:

```
license-server port port
```

Example:
```
ciscoasa(config)# license-server port 40000
```

The *port* is between 1 and 65535. The default is TCP port 50554.

**Step 4** (Optional) Identify the backup server IP address and serial number:

```
license-server backup address backup-id serial_number [ha-backup-id ha_serial_number]
```

Example:
```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
```

If the backup server is part of a failover pair, identify the standby unit serial number as well. You can only identify 1 backup server and its optional standby unit.

**Step 5**
Enable this unit to be the shared licensing server:

```
license-server enable interface_name
```

Example:
```
ciscoasa(config)# license-server enable inside
```
Configure a Shared License

Specify the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

Examples
The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
JMX1378B9W3
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378B9W3
ciscoasa(config)# license-server enable inside
JMX1378B9W3
ciscoasa(config)# license-server enable dmz
```

Configure the Shared Licensing Backup Server (Optional)

This section enables a shared license participant to act as the backup server if the main server goes down.

Before You Begin
The backup server must have a shared licensing participant key.

Procedure

Step 1
Identify the shared licensing server IP address and shared secret:

```
license-server address address secret secret [port port]
```

Example:
```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

If you changed the default port in the server configuration, set the port for the backup server to match.

Step 2
Enable this unit to be the shared licensing backup server:

```
license-server backup enable [interface_name]
```

Example:
```
ciscoasa(config)# license-server backup enable inside
```

Specify the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

Examples
The following example identifies the license server and shared secret, and enables this unit as the backup shared license server on the inside interface and dmz interface:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```
Configure the Shared Licensing Participant

This section configures a shared licensing participant to communicate with the shared licensing server.

Before You Begin
The participant must have a shared licensing participant key.

Procedure

Step 1
Identify the shared licensing server IP address and shared secret:

```
license-server address address secret secret [port port]
```

Example:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

If you changed the default port in the server configuration, set the port for the participant to match.

Step 2
(Optional) If you configured a backup server, enter the backup server address:

```
license-server backup address address
```

Example:

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

Examples
The following example sets the license server IP address and shared secret, as well as the backup license server IP address:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```
```
ciscoasa(config)# license-server backup address 10.1.1.2
```

Monitoring PAK Licenses

This section describes how to view license information.

- Viewing Your Current License, page 3-38
- Monitoring the Shared License, page 3-49

Viewing Your Current License

This section describes how to view your current license, and for time-based activation keys, how much time the license has left.

Before You Begin
If you have a No Payload Encryption model, then you view the license, VPN and Unified Communications licenses will not be listed. See No Payload Encryption Models, page 3-27 for more information.
Procedure

Step 1  Show the permanent license, active time-based licenses, and the running license, which is a combination of the permanent license and active time-based licenses:

```
show activation-key [detail]
```

The `detail` keyword also shows inactive time-based licenses.

For failover or cluster units, this command also shows the “cluster” license, which is the combined keys of all units.

Examples

**Example 3-1  Standalone Unit Output for the show activation-key command**

The following is sample output from the `show activation-key` command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as each active time-based license:

```
ciscoasa# show activation-key
Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLAGs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
Shared AnyConnect Premium Peers   : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment       : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter : Enabled   646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions : 10        62 days
```
Example 3-2  Standalone Unit Output for show activation-key detail

The following is sample output from the show activation-key detail command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as the permanent license and each installed time-based license (active and inactive):

ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25  perpetual
Total VPN Peers                  : 25  perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions          : 2              perpetual
Total UC Proxy Sessions          : 2              perpetual
Botnet Traffic Filter            : Enabled 39 days
Intercompany Media Engine        : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25  perpetual
Total VPN Peers                  : 25  perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions          : 2              perpetual
Total UC Proxy Sessions          : 2              perpetual
Botnet Traffic Filter            : Enabled 39 days
Intercompany Media Engine        : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
Example 3-3 Primary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the `show activation-key detail` command for the primary failover unit that shows:

- The primary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The primary unit permanent license.
- The primary unit installed time-based licenses (active and inactive).

```
ciscoasa# show activation-key detail
Serial Number: P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 150 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
Security Contexts : 12 perpetual
GTP/GPRS : Enabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Enabled 33 days
Intercompany Media Engine : Disabled perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 150 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
Security Contexts : 12 perpetual
GTP/GPRS : Enabled perpetual
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
```
Monitoring PAK Licenses

Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Enabled 33 days
Intercompany Media Engine : Disabled perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANS : 150 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Disabled perpetual
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter : Enabled 33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts : 2 7 days
AnyConnect Premium Peers : 100 7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions : 100 14 days

Example 3-4  Secondary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the show activation-key detail command for the secondary failover unit that shows:

- The secondary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The secondary unit permanent license.
- The secondary installed time-based licenses (active and inactive). This unit does not have any time-based licenses, so none display in this sample output.

```
ciscoasa# show activation-key detail
Serial Number: P3000000111
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANS : 150 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Disabled perpetual
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
This platform has an ASA 5520 VPN Plus license.
Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANS : 150 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
Security Contexts : 10 perpetual
GTP/GPRS : Enabled perpetual
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Enabled 33 days
Intercompany Media Engine : Disabled perpetual
This platform has an ASA 5520 VPN Plus license.
Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANS : 150 perpetual
Inside Hosts : Unlimited perpetual
```
Monitoring PAK Licenses

Chapter 3      Product Authorization Key Licenses

Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Disabled perpetual
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual

The flash permanent activation key is the SAME as the running permanent key.

Example 3-5  Standalone Unit Output for the ASAv without a License for show activation-key

The following output for a deployed 1 vCPU ASAv shows a blank activation key, an Unlicensed status, and a message to install a 1 vCPU license.

Note

The command output shows, “This platform has an ASAv VPN Premium license.” This message specifies that the ASAv can perform payload encryption; it does not refer to the ASAv Standard vs. Premium licenses.

ciscoasa# show activation-key
Serial Number: 9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs : 0 perpetual
Maximum Physical Interfaces : 10 perpetual
Maximum VLANs : 50 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Standby perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 0 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Enabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster: Disabled perpetual

This platform has an ASAv VPN Premium license.

Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.

Example 3-6  Standalone Unit Output for the ASAv with a 4 vCPU Standard License for show activation-key

The command output shows, “This platform has an ASAv VPN Premium license.” This message specifies that the ASAv can perform payload encryption; it does not refer to the ASAv Standard vs. Premium licenses.

ciscoasa# show activation-key
Serial Number: 9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs: 4 perpetual
Maximum Physical Interfaces: 10 perpetual
Maximum VLANs: 200 perpetual
Inside Hosts: Unlimited perpetual
Failover: Active/Standby perpetual
Encryption-DES: Enabled perpetual
Encryption-3DES-AES: Enabled perpetual
Security Contexts: 0 perpetual
GTP/GPRS: Enabled perpetual
AnyConnect Premium Peers: 2 perpetual
AnyConnect Essentials: Disabled perpetual
Other VPN Peers: 750 perpetual
Total VPN Peers: 750 perpetual
Shared License: Disabled perpetual
AnyConnect for Mobile: Disabled perpetual
AnyConnect for Cisco VPN Phone: Disabled perpetual
Advanced Endpoint Assessment: Disabled perpetual
UC Phone Proxy Sessions: 1000 perpetual
Total UC Proxy Sessions: 1000 perpetual
Botnet Traffic Filter: Enabled perpetual
Intercompany Media Engine: Enabled perpetual
Cluster: Disabled perpetual

This platform has an ASAv VPN Premium license.
The flash permanent activation key is the SAME as the running permanent key.

Example 3-7  Standalone Unit Output for the ASAv with a 4 vCPU Premium License for show activation-key

The command output shows, “This platform has an ASAv VPN Premium license.” This message specifies that the ASAv can perform payload encryption; it does not refer to the ASAv Standard vs. Premium licenses.

ciscoasa# show activation-key
Serial Number: 9ALQ8W1XCJ7
Monitoring PAK Licenses

Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82

ASA Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs : 4 perpetual
Maximum Physical Interfaces : 10 perpetual
Maximum VLANs : 200 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Standby perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 0 perpetual
GTP/GPRS : Enabled perpetual
AnyConnect Premium Peers : 750 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Enabled perpetual
AnyConnect for Cisco VPN Phone : Enabled perpetual
Advanced Endpoint Assessment : Enabled perpetual
UC Phone Proxy Sessions : 1000 perpetual
Total UC Proxy Sessions : 1000 perpetual
Botnet Traffic Filter : Enabled perpetual
Intercompany Media Engine : Enabled perpetual
Cluster : Disabled perpetual

This platform has an ASA VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#

Example 3-8 Primary Unit Output for the ASA Services Module in a Failover Pair for show activation-key

The following is sample output from the `show activation-key` command for the primary failover unit that shows:

- The primary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The primary unit installed time-based licenses (active and inactive).
ciscoasa# show activation-key

Serial Number: SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces : 1024 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
DES : Enabled perpetual
3DES-AES : Enabled perpetual
Security Contexts : 25 perpetual
GTP/GPRS : Enabled perpetual
Botnet Traffic Filter : Enabled 330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

Failover cluster licensed features for this platform:
- Maximum Interfaces: 1024, perpetual
- Inside Hosts: Unlimited, perpetual
- Failover: Active/Active, perpetual
- DES: Enabled, perpetual
- 3DES-AES: Enabled, perpetual
- Security Contexts: 50, perpetual
- GTP/GPRS: Enabled, perpetual
- Botnet Traffic Filter: Enabled, 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter: Enabled, 330 days

**Example 3-9 Secondary Unit Output for the ASA Services Module in a Failover Pair for show activation-key**

The following is sample output from the `show activation-key` command for the secondary failover unit that shows:

- The secondary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The secondary installed time-based licenses (active and inactive). This unit does not have any time-based licenses, so none display in this sample output.

ciscoasa# show activation-key detail

Serial Number: SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
- Maximum Interfaces: 1024, perpetual
- Inside Hosts: Unlimited, perpetual
- Failover: Active/Active, perpetual
- DES: Enabled, perpetual
- 3DES-AES: Enabled, perpetual
- Security Contexts: 25, perpetual
- GTP/GPRS: Disabled, perpetual
- Botnet Traffic Filter: Disabled, perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

Failover cluster licensed features for this platform:
- Maximum Interfaces: 1024, perpetual
- Inside Hosts: Unlimited, perpetual
- Failover: Active/Active, perpetual
- DES: Enabled, perpetual
- 3DES-AES: Enabled, perpetual
- Security Contexts: 50, perpetual
Monitoring PAK Licenses

GTP/GPRS                        : Enabled perpetual
Botnet Traffic Filter          : Enabled 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Example 3-10 Output in a Cluster for show activation-key

ciscoasa# show activation-key
Serial Number: JMX1504L2TD
Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 4 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.
The flash permanent activation key is the same as the running permanent key.

**Monitoring the Shared License**

To monitor the shared license, enter one of the following commands.

- `show shared license [detail | client [hostname] | backup]`

  Shows shared license statistics. Optional keywords are available only for the licensing server: the `detail` keyword shows statistics per participant. To limit the display to one participant, use the `client` keyword. The `backup` keyword shows information about the backup server.

  To clear the shared license statistics, enter the `clear shared license` command.

The following is sample output from the `show shared license` command on the license participant:

```
ciscoasa> show shared license
Primary License Server : 10.3.32.20
Version              : 1
Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network : 5000
    Available         : 5000
    Utilized          : 0

  This device:
    Platform limit    : 250
    Current usage     : 0
    High usage        : 0

  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

The following is sample output from the `show shared license detail` command on the license server:

```
ciscoasa> show shared license detail
Backup License Server Info:
  Device ID           : ABCD
  Address             : 10.1.1.2
  Registered          : NO
  HA peer ID          : EFGH
  Registered          : NO

  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

  Shared license utilization:
    SSLVPN:
      Total for network : 500
      Available         : 500
      Utilized          : 0

      This device:
        Platform limit    : 250
        Current usage     : 0
        High usage        : 0

      Messages Tx/Rx/Error:
        Registration    : 0 / 0 / 0
```
History for PAK Licenses

- `show activation-key`
  Shows the licenses installed on the ASA. The `show version` command also shows license information.

- `show vpn-sessiondb`
  Shows license information about VPN sessions.

### History for PAK Licenses

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased Connections and VLANs</td>
<td>7.0(5)</td>
<td>Increased the following limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Base license connections from 32000 to 5000; VLANs from 0 to 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Security Plus license connections from 64000 to 130000; VLANs from 10 to 25.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5520 connections from 130000 to 280000; VLANs from 25 to 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5540 connections from 280000 to 400000; VLANs from 100 to 200.</td>
</tr>
<tr>
<td>SSL VPN Licenses</td>
<td>7.1(1)</td>
<td>SSL VPN licenses were introduced.</td>
</tr>
<tr>
<td>Increased SSL VPN Licenses</td>
<td>7.2(1)</td>
<td>A 5000-user SSL VPN license was introduced for the ASA 5550 and above.</td>
</tr>
<tr>
<td>Increased interfaces for the Base license on the ASA 5510</td>
<td>7.2(2)</td>
<td>For the Base license on the ASA 5510, the maximum number of interfaces was increased from 3 plus a management interface to unlimited interfaces.</td>
</tr>
</tbody>
</table>
Chapter 3  Product Authorization Key Licenses

History for PAK Licenses

Increased VLANs

- **Platform Releases:** 7.2(2)
- **Description:** The maximum number of VLANs for the Security Plus license on the ASA 5505 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 backup interface command is still useful for an Easy VPN configuration.

- VLAN limits were also increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), the ASA 5550 (from 200 to 250).

Gigabit Ethernet Support for the ASA 5510 Security Plus License

- **Platform Releases:** 7.2(3)
- **Description:** The ASA 5510 now supports Gigabit Ethernet (1000 Mbps) for the Ethernet 0/0 and 0/1 ports with the Security Plus license. In the Base license, they continue to be used as Fast Ethernet (100 Mbps) ports. Ethernet 0/2, 0/3, and 0/4 remain as Fast Ethernet ports for both licenses.

  **Note**  The interface names remain Ethernet 0/0 and Ethernet 0/1.

- Use the `speed` command to change the speed on the interface and use the `show interface` command to see what speed is currently configured for each interface.

Advanced Endpoint Assessment License

- **Platform Releases:** 8.0(2)
- **Description:** The Advanced Endpoint Assessment license was introduced. As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connections, 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).

- With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements.

- 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.

VPN Load Balancing for the ASA 5510

- **Platform Releases:** 8.0(2)
- **Description:** VPN load balancing is now supported on the ASA 5510 Security Plus license.

AnyConnect for Mobile License

- **Platform Releases:** 8.0(3)
- **Description:** The AnyConnect for Mobile license was introduced. It lets Windows mobile devices connect to the ASA using the AnyConnect client.

Time-based Licenses

- **Platform Releases:** 8.0(4)/8.1(2)
- **Description:** Support for time-based licenses was introduced.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased VLANs for the ASA 5580</td>
<td>8.1(2)</td>
<td>The number of VLANs supported on the ASA 5580 are increased from 100 to 250.</td>
</tr>
<tr>
<td>Unified Communications Proxy Sessions license</td>
<td>8.0(4)</td>
<td>The UC Proxy sessions license was introduced. Phone Proxy, Presence Federation Proxy, and Encrypted Voice Inspection applications use TLS proxy sessions for their connections. Each TLS proxy session is counted against the UC license limit. All of these applications are licensed under the UC Proxy umbrella, and can be mixed and matched. This feature is not available in Version 8.1.</td>
</tr>
<tr>
<td>Botnet Traffic Filter License</td>
<td>8.2(1)</td>
<td>The Botnet Traffic Filter license was introduced. The Botnet Traffic Filter protects against malware network activity by tracking connections to known bad domains and IP addresses.</td>
</tr>
<tr>
<td>AnyConnect Essentials License</td>
<td>8.2(1)</td>
<td>The AnyConnect Essentials License was introduced. This license enables AnyConnect VPN client access to the ASA. This license does not support browser-based SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium license instead of the AnyConnect Essentials license. Note With the AnyConnect Essentials license, VPN users can use a Web browser to log in, and download and start (WebLaunch) the AnyConnect client. The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium license. The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given ASA: AnyConnect Premium license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium licenses on different ASAs in the same network. By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the <code>webvpn</code>, and then the <code>no anyconnect-essentials</code> command.</td>
</tr>
<tr>
<td>SSL VPN license changed to AnyConnect Premium SSL VPN Edition license</td>
<td>8.2(1)</td>
<td>The SSL VPN license name was changed to the AnyConnect Premium SSL VPN Edition license.</td>
</tr>
<tr>
<td>Shared Licenses for SSL VPN</td>
<td>8.2(1)</td>
<td>Shared licenses for SSL VPN were introduced. Multiple ASAs can share a pool of SSL VPN sessions on an as-needed basis.</td>
</tr>
<tr>
<td>Mobility Proxy application no longer requires Unified Communications Proxy license</td>
<td>8.2(2)</td>
<td>The Mobility Proxy no longer requires the UC Proxy license.</td>
</tr>
</tbody>
</table>
### Chapter 3  Product Authorization Key Licenses

#### History for PAK Licenses

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 GE I/O license for the ASA 5585-X with SSP-20</td>
<td>8.2(3)</td>
<td>We introduced the 10 GE I/O license for the ASA 5585-X with SSP-20 to enable 10-Gigabit Ethernet speeds for the fiber ports. The SSP-60 supports 10-Gigabit Ethernet speeds by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The ASA 5585-X is not supported in 8.3(x).</td>
</tr>
<tr>
<td>10 GE I/O license for the ASA 5585-X with SSP-10</td>
<td>8.2(4)</td>
<td>We introduced the 10 GE I/O license for the ASA 5585-X with SSP-10 to enable 10-Gigabit Ethernet speeds for the fiber ports. The SSP-40 supports 10-Gigabit Ethernet speeds by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The ASA 5585-X is not supported in 8.3(x).</td>
</tr>
<tr>
<td>Non-identical failover licenses</td>
<td>8.3(1)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following commands: <code>show activation-key</code> and <code>show version</code>.</td>
</tr>
<tr>
<td>Stackable time-based licenses</td>
<td>8.3(1)</td>
<td>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 stack time-based licenses so that you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early.</td>
</tr>
<tr>
<td>Intercompany Media Engine License</td>
<td>8.3(1)</td>
<td>The IME license was introduced.</td>
</tr>
<tr>
<td>Multiple time-based licenses active at the same time</td>
<td>8.3(1)</td>
<td>You can now install multiple time-based licenses, and have one license per feature active at a time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following commands: <code>show activation-key</code> and <code>show version</code>.</td>
</tr>
<tr>
<td>Discrete activation and deactivation of time-based licenses.</td>
<td>8.3(1)</td>
<td>You can now activate or deactivate time-based licenses using a command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following commands: `activation-key [activate</td>
</tr>
<tr>
<td>AnyConnect Premium SSL VPN Edition license changed to AnyConnect Premium SSL VPN license</td>
<td>8.3(1)</td>
<td>The AnyConnect Premium SSL VPN Edition license name was changed to the AnyConnect Premium SSL VPN license.</td>
</tr>
</tbody>
</table>
### History for PAK Licenses

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Payload Encryption image for export</td>
<td>8.3(2)</td>
<td>If you install the No Payload Encryption software on the ASA 5505 through 5550, then you disable Unified Communications, strong encryption VPN, and strong encryption management protocols.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This special image is only supported in 8.3(x); for No Payload Encryption support in 8.4(1) and later, you need to purchase a special hardware version of the ASA.</td>
</tr>
<tr>
<td>Increased contexts for the ASA 5550, 5580, and 5585-X</td>
<td>8.4(1)</td>
<td>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.</td>
</tr>
<tr>
<td>Increased VLANs for the ASA 5580 and 5585-X</td>
<td>8.4(1)</td>
<td>For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.</td>
</tr>
<tr>
<td>Increased connections for the ASA 5580 and 5585-X</td>
<td>8.4(1)</td>
<td>We increased the firewall connection limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5580-20—1,000,000 to 2,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5580-40—2,000,000 to 4,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-10: 750,000 to 1,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-20: 1,000,000 to 2,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-40: 2,000,000 to 4,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.</td>
</tr>
<tr>
<td>AnyConnect Premium SSL VPN license changed to AnyConnect Premium license</td>
<td>8.4(1)</td>
<td>The AnyConnect Premium SSL VPN license name was changed to the AnyConnect Premium license. The license information display was changed from “SSL VPN Peers” to “AnyConnect Premium Peers.”</td>
</tr>
<tr>
<td>Increased AnyConnect VPN sessions for the ASA 5580</td>
<td>8.4(1)</td>
<td>The AnyConnect VPN session limit was increased from 5,000 to 10,000.</td>
</tr>
<tr>
<td>Increased Other VPN sessions for the ASA 5580</td>
<td>8.4(1)</td>
<td>The other VPN session limit was increased from 5,000 to 10,000.</td>
</tr>
<tr>
<td>IPsec remote access VPN using IKEv2</td>
<td>8.4(1)</td>
<td>IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The following limitation exists in our support for IKEv2 on the ASA:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We currently do not support duplicate security associations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IKEv2 site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). The Other VPN license is included in the Base license.</td>
</tr>
<tr>
<td>No Payload Encryption hardware for export</td>
<td>8.4(1)</td>
<td>For models available with No Payload Encryption (for example, the ASA 5585-X), the ASA software disables Unified Communications and VPN features, making the ASA available for export to certain countries.</td>
</tr>
</tbody>
</table>

---

**Feature Name**

<table>
<thead>
<tr>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Payload Encryption image for export</td>
<td>If you install the No Payload Encryption software on the ASA 5505 through 5550, then you disable Unified Communications, strong encryption VPN, and strong encryption management protocols.</td>
</tr>
<tr>
<td>Increased contexts for the ASA 5550, 5580, and 5585-X</td>
<td>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.</td>
</tr>
<tr>
<td>Increased VLANs for the ASA 5580 and 5585-X</td>
<td>For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.</td>
</tr>
<tr>
<td>Increased connections for the ASA 5580 and 5585-X</td>
<td>We increased the firewall connection limits:</td>
</tr>
<tr>
<td></td>
<td>• ASA 5580-20—1,000,000 to 2,000,000.</td>
</tr>
<tr>
<td></td>
<td>• ASA 5580-40—2,000,000 to 4,000,000.</td>
</tr>
<tr>
<td></td>
<td>• ASA 5585-X with SSP-10: 750,000 to 1,000,000.</td>
</tr>
<tr>
<td></td>
<td>• ASA 5585-X with SSP-20: 1,000,000 to 2,000,000.</td>
</tr>
<tr>
<td></td>
<td>• ASA 5585-X with SSP-40: 2,000,000 to 4,000,000.</td>
</tr>
<tr>
<td></td>
<td>• ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.</td>
</tr>
<tr>
<td>AnyConnect Premium SSL VPN license changed to AnyConnect Premium license</td>
<td>The AnyConnect Premium SSL VPN license name was changed to the AnyConnect Premium license. The license information display was changed from “SSL VPN Peers” to “AnyConnect Premium Peers.”</td>
</tr>
<tr>
<td>Increased AnyConnect VPN sessions for the ASA 5580</td>
<td>The AnyConnect VPN session limit was increased from 5,000 to 10,000.</td>
</tr>
<tr>
<td>Increased Other VPN sessions for the ASA 5580</td>
<td>The other VPN session limit was increased from 5,000 to 10,000.</td>
</tr>
<tr>
<td>IPsec remote access VPN using IKEv2</td>
<td>IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The following limitation exists in our support for IKEv2 on the ASA: We currently do not support duplicate security associations.</td>
</tr>
<tr>
<td></td>
<td>IKEv2 site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). The Other VPN license is included in the Base license.</td>
</tr>
<tr>
<td>No Payload Encryption hardware for export</td>
<td>For models available with No Payload Encryption (for example, the ASA 5585-X), the ASA software disables Unified Communications and VPN features, making the ASA available for export to certain countries.</td>
</tr>
</tbody>
</table>
### History for PAK Licenses

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual SSPs for SSP-20 and SSP-40</td>
<td>8.4(2)</td>
<td>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. When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled.</td>
</tr>
<tr>
<td>IPS Module license for the ASA 5512-X through ASA 5555-X</td>
<td>8.6(1)</td>
<td>The IPS SSP software module on the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X requires the IPS module license.</td>
</tr>
<tr>
<td>Clustering license for the ASA 5580 and ASA 5585-X.</td>
<td>9.0(1)</td>
<td>A clustering license was added for the ASA 5580 and ASA 5585-X.</td>
</tr>
<tr>
<td>Support for VPN on the ASASM</td>
<td>9.0(1)</td>
<td>The ASASM now supports all VPN features.</td>
</tr>
<tr>
<td>Unified communications support on the ASASM</td>
<td>9.0(1)</td>
<td>The ASASM now supports all Unified Communications features.</td>
</tr>
<tr>
<td>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</td>
<td>9.0(1)</td>
<td>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.</td>
</tr>
<tr>
<td>Support for 16 cluster members for the ASA 5585-X</td>
<td>9.2(1)</td>
<td>The ASA 5585-X now supports 16-unit clusters.</td>
</tr>
<tr>
<td>ASAv4 and ASAv30 Standard and Premium model licenses introduced</td>
<td>9.2(1)</td>
<td>The ASAv was introduced with a simple licensing scheme: ASAv4 and ASAv30 permanent licenses in Standard or Premium levels. No add-on licenses are available.</td>
</tr>
</tbody>
</table>
Smart Software Licensing for the ASAv

9.3(2) and Later
Cisco Smart Software Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAvs without having to manage each unit’s license key. Smart Software Licensing also lets you see your license usage and needs at a glance.

- Supported Licenses, page 4-1
- About Smart Software Licensing, page 4-4
- Prerequisites for Smart Software Licensing, page 4-6
- Guidelines for Smart Software Licensing, page 4-6
- Defaults for Smart Software Licensing, page 4-7
- Configure Smart Software Licensing, page 4-7
- Manage Smart Software Licensing, page 4-9
- Monitoring Smart Software Licensing, page 4-10
- History for Smart Software Licensing, page 4-12

Supported Licenses
This section lists the license entitlements available for the ASAv.

- ASAv5 and ASAv10, page 4-2
- ASAv30, page 4-3
- License Notes, page 4-4
### Supported Licenses

#### ASAv5 and ASAv10

**Table 4-1  ASAv5 and ASAv10 License Features**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Supported</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>100,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Supported</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Supported</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>500</td>
</tr>
</tbody>
</table>

**VPN Licenses:** For AnyConnect 4 and later, the number of simultaneous users and VPN features are controlled by the AnyConnect license, available separately. VPN licenses are enabled to the maximum level on the ASA.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>250</td>
</tr>
<tr>
<td><strong>Adv. Endpoint Assessment</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Other VPN Licenses**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>250</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>250</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**General Licenses**

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput Level</td>
<td>ASAv5: 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>ASAv10: 1 Gbps</td>
</tr>
<tr>
<td>Encryption</td>
<td>Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>716</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
</tr>
<tr>
<td>Clustering</td>
<td>No support</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>50</td>
</tr>
<tr>
<td>RAM, vCPUs, vCPU Frequency Limit</td>
<td>2 GB, 1 vCPU, 5000 MHz</td>
</tr>
</tbody>
</table>
### ASA30

<table>
<thead>
<tr>
<th>License Features</th>
<th>Standard License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Supported</td>
</tr>
<tr>
<td>Firewall Conn, Concurrent</td>
<td>500,000</td>
</tr>
<tr>
<td>GTP/GPRS</td>
<td>Supported</td>
</tr>
<tr>
<td>Intercompany Media Eng.</td>
<td>Supported</td>
</tr>
<tr>
<td>UC Phone Proxy Sessions, Total UC Proxy Sessions</td>
<td>1000</td>
</tr>
<tr>
<td><strong>VPN Licenses:</strong> For AnyConnect 4 and later, the number of simultaneous users and VPN features are controlled by the AnyConnect license, available separately. VPN licenses are enabled to the maximum level on the ASA.</td>
<td></td>
</tr>
<tr>
<td>AnyConnect Premium Peers (maximum)</td>
<td>750</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Shared licenses: No Support. AnyConnect 4 licenses are shared and no longer require a shared server or participant license.</td>
</tr>
<tr>
<td>Adv. Endpoint Assessment</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>Enabled</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>Disabled</td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Other VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>750</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>750</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Throughput Level</td>
<td>2 Gbps</td>
</tr>
<tr>
<td>Encryption</td>
<td>Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby</td>
</tr>
<tr>
<td>Interfaces of all types, Max.</td>
<td>1316</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
</tr>
<tr>
<td>Clustering</td>
<td>No support</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>200</td>
</tr>
<tr>
<td>RAM, vCPUs, vCPU Frequency Limit</td>
<td>8 GB, 4 vCPUs, 20000 MHz</td>
</tr>
<tr>
<td><strong>Note:</strong> If you choose to deploy 2 or 3 vCPUs, then see the following values:</td>
<td></td>
</tr>
<tr>
<td>2 vCPUs—4 GB RAM, vCPU Frequency Limit of 10000 MHz, 250,000 concurrent firewall connections.</td>
<td></td>
</tr>
<tr>
<td>3 vCPUs—4 GB RAM, vCPU Frequency Limit of 15000 MHz, 350,000 concurrent firewall connections.</td>
<td></td>
</tr>
</tbody>
</table>
License Notes

The following table includes additional information about licenses.

Table 4-3 License Notes

<table>
<thead>
<tr>
<th>License</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium</td>
<td>AnyConnect Premium sessions include the following VPN types:</td>
</tr>
<tr>
<td></td>
<td>- SSL VPN</td>
</tr>
<tr>
<td></td>
<td>- Clientless SSL VPN</td>
</tr>
<tr>
<td></td>
<td>- IPsec remote access VPN using IKEv2</td>
</tr>
<tr>
<td>Encryption</td>
<td>The DES license cannot be disabled. Although the 3DES license is</td>
</tr>
<tr>
<td></td>
<td>installed, DES is still available. To prevent the use of DES when</td>
</tr>
<tr>
<td></td>
<td>you want to only use strong encryption, be sure to configure any</td>
</tr>
<tr>
<td></td>
<td>relevant commands to use only strong encryption.</td>
</tr>
<tr>
<td>Interfaces of all types,</td>
<td>The maximum number of combined interfaces; for example, VLANs,</td>
</tr>
<tr>
<td>Max.</td>
<td>physical, redundant, bridge group, and EtherChannel interfaces. Every</td>
</tr>
<tr>
<td></td>
<td>interface command defined in the configuration counts against this</td>
</tr>
<tr>
<td></td>
<td>limit. For example, both of the following interfaces count even if</td>
</tr>
<tr>
<td></td>
<td>the GigabitEthernet 0/0 interface is defined as part of port-channel</td>
</tr>
<tr>
<td></td>
<td>1:</td>
</tr>
<tr>
<td></td>
<td>interface gigabitethernet 0/0</td>
</tr>
<tr>
<td></td>
<td>and</td>
</tr>
<tr>
<td></td>
<td>interface port-channel 1</td>
</tr>
<tr>
<td>Other VPN</td>
<td>Other VPN sessions include the following VPN types:</td>
</tr>
<tr>
<td></td>
<td>- IPsec remote access VPN using IKEv1</td>
</tr>
<tr>
<td></td>
<td>- IPsec site-to-site VPN using IKEv1</td>
</tr>
<tr>
<td></td>
<td>- IPsec site-to-site VPN using IKEv2</td>
</tr>
<tr>
<td>Total VPN (sessions),</td>
<td>- Although the maximum VPN sessions add up to more than the</td>
</tr>
<tr>
<td>combined all types</td>
<td>maximum VPN AnyConnect and Other VPN sessions, the combined sessions</td>
</tr>
<tr>
<td></td>
<td>should not exceed the VPN session limit. If you exceed the maximum</td>
</tr>
<tr>
<td></td>
<td>VPN sessions, you can overload the ASA, so be sure to size your</td>
</tr>
<tr>
<td></td>
<td>network appropriately.</td>
</tr>
<tr>
<td></td>
<td>- If you start a clientless SSL VPN session and then start an</td>
</tr>
<tr>
<td></td>
<td>AnyConnect client session from the portal, 1 session is used in</td>
</tr>
<tr>
<td></td>
<td>total. However, if you start the AnyConnect client first (from a</td>
</tr>
<tr>
<td></td>
<td>standalone client, for example) and then log into the clientless SSL</td>
</tr>
<tr>
<td></td>
<td>VPN portal, then 2 sessions are used.</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>For an interface to count against the VLAN limit, you must assign a</td>
</tr>
<tr>
<td></td>
<td>VLAN to it. For example:</td>
</tr>
<tr>
<td></td>
<td>interface gigabitethernet 0/0.100</td>
</tr>
<tr>
<td></td>
<td>vlan 100</td>
</tr>
</tbody>
</table>

About Smart Software Licensing

This section describes how Smart Software Licensing works with the ASAv.

- Cisco Smart Software Manager and Accounts, page 4-5
- Licenses and Devices Managed per Virtual Account, page 4-5
- Device Registration and Tokens, page 4-5
Cisco Smart Software Licensing for the ASAv

When you purchase 1 or more licenses for the ASAv, you manage them in the Cisco Smart Software Manager:

http://tools.cisco.com/rhodui/index

The Smart Software Manager lets you create a master account for your organization.

By default, your licenses are assigned to the Default Virtual Account under your master account. As the account administrator, you can optionally create additional virtual accounts; for example, you can create accounts for regions, departments, or subsidiaries. Multiple virtual accounts let you more easily manage large numbers of licenses and devices.

Licenses and Devices Managed per Virtual Account

Licenses and devices are managed per virtual account: only that virtual account’s ASAvs can use the licenses assigned to the account. If you need additional licenses, you can transfer an unused license from another virtual account. You can also transfer ASAvs between virtual accounts.

Device Registration and Tokens

For each virtual account, you can create a registration token. This token is valid for 30 days by default. Enter this token ID plus entitlement levels when you deploy each ASAv, or when you register an existing ASAv. You can create a new token if an existing token is expired.

At startup after deployment, or after you manually configure these parameters on an existing ASAv, the ASAv registers with the Cisco License Authority. When the ASAv registers with the token, the License Authority issues an ID certificate for communication between the device and the License Authority. This certificate is valid for 1 year, although it will be renewed every 6 months.

Periodic Communication with the License Authority

The ASAv communicates with the License Authority every 30 days. If you make changes in the Smart Software Manager, you can refresh the authorization on the ASAv so the change takes place immediately. Or you can wait for the ASAv to communicate as scheduled.

You can optionally configure an HTTP proxy. Your ASAvs must have Internet access either directly or through an HTTP proxy at least every 90 days. Normal license communication occurs every 30 days, but with the grace period, your ASAv will operate for up to 90 days without calling home. You must contact the Licensing Authority before 90 days have passed.

Note

Offline licensing is not supported.
Out-of-Compliance State

The ASAv can become out of compliance in the following situations:

- Over-utilization—When the ASAv uses unavailable licenses.
- License expiration—When a time-based license expires.
- Lack of communication—When the ASAv cannot reach the Licensing Authority for re-authorization.

After 90 days of reauthorization attempts, the ASAv will be severely rate-limited until you are able to successfully reauthorize.

Smart Call Home Infrastructure

By default, a Smart Call Home profile exists in the configuration called “License”. This profile specifies the URL for the Licensing Authority. You cannot remove this profile. Note that the only configurable option for the License profile is the destination address URL for the License Authority. Unless directed by Cisco TAC, you should not change the License Authority URL.

You cannot disable Smart Call Home for Smart Software Licensing; for example, even if you disable Smart Call Home using the no service call-home command, Smart Software Licensing is not disabled. Other Smart Call Home functions are not turned on unless you specifically configure them.

Prerequisites for Smart Software Licensing

- Create a master account on the Cisco Smart Software Manager: http://tools.cisco.com/rhodui/index
- Purchase 1 or more ASAv licenses from Cisco Software Central.
- Ensure Internet access or HTTP proxy access from the ASAv, so the ASAv can contact the Licensing Authority. Offline licensing is not supported.
- Configure a DNS server so the ASA can resolve the name of the licensing authority server. See Configure the DNS Server, page 16-14.

Guidelines for Smart Software Licensing

Failover

You must deploy both units with the same model license.

Additional Guidelines

You cannot use PAK-based licensing with the ASAv. Only Smart Software Licensing is supported. If you upgrade an existing PAK-licensed ASAv, then the previously installed activation key will be ignored, but retained on the device. If you downgrade the ASAv, the activation key will be reinstated.
Chapter 4  Smart Software Licensing for the ASAv

Defaults for Smart Software Licensing

- The ASAv default configuration includes a Smart Call Home profile called “License” that specifies the URL for the Licensing Authority.

```bash
call-home
  profile License
    destination address http
    https://tools.cisco.com/lts/service/oddce/services/DDCEService
```

- When you deploy the ASAv, you set the feature tier and throughput level. Only the standard level is available at this time.

```bash
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
```

- Also during deployment, you can optionally configure an HTTP proxy.

```bash
call-home
  http-proxy ip_address port port
```

Configure Smart Software Licensing

When you deploy the ASAv, the device registers with the License Authority, and Smart Software Licensing is enabled according to the values you enter at deployment. If you need to change your license entitlement or configure Smart Software Licensing for an existing ASAv, perform the following tasks.

**Step 1** (Optional) Configure the HTTP Proxy, page 4-7.

**Step 2** Set the Smart License Entitlement, page 4-8.

**Step 3** Register the ASAv with the License Authority, page 4-8.

(Optional) Configure the HTTP Proxy

If your network uses an HTTP proxy for Internet access, you must configure the proxy address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

**Procedure**

**Step 1** Specify the HTTP Proxy URL:

```bash
call-home
  http-proxy ip_address port port
```

Example:

```bash
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```
Set the Smart License Entitlement

To request the license entitlement, perform the following procedure.

**Procedure**

**Step 1** Enter license smart configuration mode:

```bash
license smart
```

Example:

```bash
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

**Step 2** Set the feature tier:

```bash
feature tier standard
```

Only the standard tier is available.

**Step 3** Set the throughput level:

```bash
throughput level {100M | 1G | 2G}
```

Example:

```bash
ciscoasa(config-smart-lic)# throughput level 2G
```

**Step 4** Exit license smart mode to apply your changes:

```bash
exit
```

Example:

```bash
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Your changes do not take effect until you exit the license smart configuration mode, either by explicitly exiting the mode (**exit or end**) or by entering any command that takes you to a different mode.

Register the ASAv with the License Authority

When you register the ASAv, the License Authority issues an ID certificate for communication between the ASAv and the License Authority. It also assigns the ASAv to the appropriate virtual account. Normally, this procedure is a one-time instance. However, you might need to later re-register the ASAv if the ID certificate expires because of a communication problem, for example.

**Procedure**

**Step 1** In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this ASAv.

**Step 2** Enter the registration token on the ASAv:

```bash
license smart register idtoken id_token [force]
```
Example:

ciscoasa# license smart register idtoken
YjE3Njc5MzYtMGQzMi00OTA4LWJhODItNzBhMGQtOGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQkdYRmZ1N1NCG1vRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A

Use the **force** keyword to register an ASAv that is already registered, but that might be out of sync with the License Authority. For example, use **force** if the ASAv was accidentally removed from the Smart Software Manager.

The ASAv attempts to register with the License Authority and request authorization for the configured license entitlements.

---

**Step 3**

### Manage Smart Software Licensing

You might need to deregister an ASAv from your account or manually renew the ID certificate or license entitlement.

- Deregister the ASAv, page 4-9
- Renew the ID Certificate or License Entitlement, page 4-9

### Deregister the ASAv

Deregistering the ASAv removes the ASAv from your account. All license entitlements and certificates on the ASAv are removed. You might want to deregister to free up a license for a new ASAv. Alternatively, you can remove the ASAv from the Smart Software Manager.

**Procedure**

**Step 1**

Deregister the ASAv:

`license smart deregister`

---

### Renew the ID Certificate or License Entitlement

By default, the ID certificate is automatically renewed every 6 months, and the license entitlement is renewed every 30 days. You might want to manually renew the registration for either of these items if you have a limited window for Internet access, or if you make any licensing changes in the Smart Software Manager, for example.

**Procedure**

**Step 1**

Renew the ID certificate:

`license smart renew id`
Monitoring Smart Software Licensing

You can monitor the license features, status, and certificate, as well as enable debug messages.

- Viewing Your Current License, page 4-10
- Viewing Smart License Status, page 4-11
- Displaying ID Certificate Information, page 4-11
- Debugging Smart Software Licensing, page 4-11

Viewing Your Current License

See the following commands for viewing your license:

- `show activation-key`, `show license features`

  The following example shows an ASAv with only a base license (no current license entitlement):

  Serial Number: 9AAHGX8514R

  ASAv Platform License State: Unlicensed
  No active entitlement: no feature tier configured

  Licensed features for this platform:
  Maximum Physical Interfaces : 10 perpetual
  Maximum VLANs : 50 perpetual
  Inside Hosts : Unlimited perpetual
  Failover : Active/Standby perpetual
  Encryption-DES : Enabled perpetual
  Encryption-3DES-AES : Enabled perpetual
  Security Contexts : 0 perpetual
  GTP/GPRS : Disabled perpetual
  AnyConnect Premium Peers : 2 perpetual
  AnyConnect Essentials : Disabled perpetual
  Other VPN Peers : 250 perpetual
  Total VPN Peers : 250 perpetual
  Shared License : Disabled perpetual
  AnyConnect for Mobile : Disabled perpetual
  AnyConnect for Cisco VPN Phone : Disabled perpetual
  Advanced Endpoint Assessment : Disabled perpetual
  UC Phone Proxy Sessions : 2 perpetual
  Total UC Proxy Sessions : 2 perpetual
  Botnet Traffic Filter : Enabled perpetual
  Intercompany Media Engine : Disabled perpetual
  Cluster : Disabled perpetual

- `show license entitlement`

  Displays detailed information about each entitlement in use, its handle (i.e. integer id), its count, tag, enforcement mode (e.g. in compliance, out of compliance, etc.), version and time at which the entitlement was requested.

**Step 2** Renew the license entitlement:

```
license smart renew auth
```
Viewing Smart License Status

See the following commands for viewing license status:

- **show license all**
  Displays the state of Smart Software Licensing, Smart Agent version, UDI information, Smart Agent state, global compliance status, the entitlements status, licensing certificate information and schedule Smart Agent tasks.

- **show license registration**
  Displays the current Smart License registration status.

- **show license pool**
  Displays the entitlement pool to which this device is assigned.

Displaying ID Certificate Information

See the following command to view the license ID certificate:

- **show license cert**
  Displays the ID certificate content, date issued, and the date it expires.

Debugging Smart Software Licensing

See the following commands for debugging clustering:

- **debug license agent {error | trace | debug | all}**
  Turns on debugging from the Smart Agent.

- **debug license level**
  Turns on various levels of Smart Software Licensing Manager debugs.
## History for Smart Software Licensing

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Smart Software Licensing for the ASAv</td>
<td>9.3(2)</td>
<td>Smart Software Licensing lets you purchase and manage a pool of licenses. Unlike PAK licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAvs without having to manage each unit’s license key. Smart Software Licensing also lets you see your license usage and needs at a glance. We introduced the following commands: clear configure license, debug license agent, feature tier, http-proxy, license smart, license smart deregister, license smart register, license smart renew, show license, show running-config license, throughput level</td>
</tr>
</tbody>
</table>
Transparent or Routed Firewall Mode

This chapter describes how to set the firewall mode to routed or transparent, as well as how the firewall works in each firewall mode. This chapter also includes information about customizing the transparent firewall operation.

You can set the firewall mode independently for each context in multiple context mode.

- About the Firewall Mode, page 5-1
- Default Settings, page 5-7
- Guidelines for Firewall Mode, page 5-7
- Set the Firewall Mode, page 5-9
- Configure ARP Inspection for the Transparent Firewall, page 5-10
- Customize the MAC Address Table for the Transparent Firewall, page 5-11
- Monitoring the Transparent Firewall, page 5-13
- Examples for Firewall Mode, page 5-13
- History for the Firewall Mode, page 5-24

About the Firewall Mode

- About Routed Firewall Mode, page 5-1
- About Transparent Firewall Mode, page 5-2

About Routed Firewall Mode

In routed mode, the Cisco ASA is considered to be a router hop in the network. Routed mode supports many interfaces. Each interface is on a different subnet. You can share interfaces between contexts.

The ASA acts as a router between connected networks, and each interface requires an IP address on a different subnet. The ASA supports multiple dynamic routing protocols. However, we recommend using the advanced routing capabilities of the upstream and downstream routers instead of relying on the ASA for extensive routing needs.
About the Firewall Mode

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

- Using the Transparent Firewall in Your Network, page 5-2
- Bridge Groups, page 5-3
- Management Interface (ASA 5512-X and Higher), page 5-4
- Allowing Layer 3 Traffic, page 5-4
- Allowed MAC Addresses, page 5-5
- Passing Traffic Not Allowed in Routed Mode, page 5-5
- BPDU Handling, page 5-5
- MAC Address vs. Route Lookups, page 5-5
- ARP Inspection, page 5-6
- MAC Address Table, page 5-7

Using the Transparent Firewall in Your Network

The ASA connects the same network between its interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network.
Figure 5-1 shows a typical transparent firewall network where the outside devices are on the same subnet as the inside devices. The inside router and hosts appear to be directly connected to the outside router.

**Figure 5-1  Transparent Firewall Network**

---

**Bridge Groups**

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; traffic is not routed to another bridge group within the ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.
Figure 5-2 shows two networks connected to the ASA, which has two bridge groups.

**Management Interface (ASA 5512-X and Higher)**

In addition to each bridge group management IP address, you can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA. For more information, see Management Interface, page 9-2.

**Allowing Layer 3 Traffic**

- Unicast IPv4 and IPv6 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an ACL.

  **Note** Broadcast and multicast traffic can be passed using access rules. See the firewall configuration guide for more information.

- ARPs are allowed through the transparent firewall in both directions without an ACL. ARP traffic can be controlled by ARP inspection.
For Layer 3 traffic travelling from a low to a high security interface, an extended ACL is required on the low security interface. See the firewall configuration guide for more information.

### Allowed MAC Addresses

The following destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped.

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD
- AppleTalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF

### Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an ACL. The transparent firewall, however, can allow almost any traffic through using either an extended ACL (for IP traffic) or an EtherType ACL (for non-IP traffic).

Non-IP traffic (for example AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using an EtherType ACL.

*Note* The transparent mode ASA does not pass CDP packets or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported.

### Passing Traffic For Routed-Mode Features

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, by using an extended ACL, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV. You can also establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an extended ACL. Likewise, protocols like HSRP or VRRP can pass through the ASA.

### BPDU Handling

To prevent loops using the Spanning Tree Protocol, BPDUs are passed by default. To block BPDUs, you need to configure an EtherType ACL to deny them. If you are using failover, you might want to block BPDUs to prevent the switch port from going into a blocking state when the topology changes. See *Transparent Firewall Mode Requirements*, page 7-14 for more information.

### MAC Address vs. Route Lookups

When the ASA runs in transparent mode, the outgoing interface of a packet is determined by performing a MAC address lookup instead of a route lookup.

Route lookups, however, are necessary for the following traffic types:
• Traffic originating on the ASA—for example, if your syslog server is located on a remote network, you must use a static route so the ASA can reach that subnet.

• Traffic that is at least one hop away from the ASA with NAT enabled—the ASA needs to perform a route lookup to find the next hop gateway; you need to add a static route on the ASA for the real host address.

• Voice over IP (VoIP) and DNS traffic with inspection enabled, and the endpoint is at least one hop away from the ASA—for example, if you use the transparent firewall between a CCM and an H.323 gateway, and there is a router between the transparent firewall and the H.323 gateway, then you need to add a static route on the ASA for the H.323 gateway for successful call completion. If you enable NAT for the inspected traffic, a static route is required to determine the egress interface for the real host address that is embedded in the packet. Affected applications include:
  - CTI QBE
  - DNS
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - Skinny (SCCP)

ARP Inspection

By default, all ARP packets are allowed through the ASA. You can control the flow of ARP packets by enabling ARP inspection.

When you enable ARP inspection, the ASA compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

• If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.

• If there is a mismatch between the MAC address, the IP address, or the interface, then the ASA drops the packet.

• If the ARP packet does not match any entries in the static ARP table, then you can set the ASA to either forward the packet out all interfaces (flood), or to drop the packet.

Note

The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.
MAC Address Table

The ASA learns and builds a MAC address table in a similar way as a normal bridge or switch: when a device sends a packet through the ASA, the ASA adds the MAC address to its table. The table associates the MAC address with the source interface so that the ASA knows to send any packets addressed to the device out the correct interface.

Because the ASA is a firewall, if the destination MAC address of a packet is not in the table, the ASA does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the following packets for directly connected devices or for remote devices:

- Packets for directly connected devices—The ASA generates an ARP request for the destination IP address, so that the ASA can learn which interface receives the ARP response.
- Packets for remote devices—The ASA generates a ping to the destination IP address so that the ASA can learn which interface receives the ping reply.

The original packet is dropped.

Default Settings

The default mode is routed mode.

Transparent Mode Defaults

- By default, all ARP packets are allowed through the ASA.
- If you enable ARP inspection, the default setting is to flood non-matching packets.
- The default timeout value for dynamic MAC address table entries is 5 minutes.
- By default, each interface automatically learns the MAC addresses of entering traffic, and the ASA adds corresponding entries to the MAC address table.

Guidelines for Firewall Mode

Context Mode Guidelines

Set the firewall mode per context.

Transparent Firewall Guidelines

- In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the ASA updates the MAC address table to use the management interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the ASA will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.
- Each directly-connected network must be on the same subnet.
- Do not specify the bridge group management IP address as the default gateway for connected devices; devices need to specify the router on the other side of the ASA as the default gateway.
The default route for the transparent firewall, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from more than one bridge group network, you need to specify a static route that identifies the network from which you expect management traffic.

See Guidelines and Limitations for Transparent Mode Interfaces, page 12-4 for more guidelines.

IPv6 Guidelines
Supports IPv6.

Additional Guidelines and Limitations
- When you change firewall modes, the ASA clears the running configuration because many commands are not supported for both modes. The startup configuration remains unchanged. If you reload without saving, then the startup configuration is loaded, and the mode reverts back to the original setting. See Set the Firewall Mode, page 5-9 for information about backing up your configuration file.
- If you download a text configuration to the ASA that changes the mode with the `firewall transparent` command, be sure to put the command at the top of the configuration; the ASA changes the mode as soon as it reads the command and then continues reading the configuration you downloaded. If the command appears later in the configuration, the ASA clears all the preceding lines in the configuration. See Configuring the Images and Startup Configuration to Use, page 36-22 for information about downloading text files.

Unsupported Features in Transparent Mode
Table 5-1 lists the features are not supported in transparent mode.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic DNS</td>
<td>—</td>
</tr>
<tr>
<td>DHCP relay</td>
<td>The transparent firewall can act as a DHCP server, but it does not support the DHCP relay commands. DHCP relay is not required because you can allow DHCP traffic to pass through using two extended ACLs: one that allows DHCP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.</td>
</tr>
<tr>
<td>Dynamic routing protocols</td>
<td>You can, however, add static routes for traffic originating on the ASA. You can also allow dynamic routing protocols through the ASA using an extended ACL.</td>
</tr>
<tr>
<td>Multicast IP routing</td>
<td>You can allow multicast traffic through the ASA by allowing it in an extended ACL.</td>
</tr>
<tr>
<td>QoS</td>
<td>—</td>
</tr>
</tbody>
</table>
Chapter 5  Transparent or Routed Firewall Mode

Set the Firewall Mode

This section describes how to change the firewall mode. We recommend that you set the firewall mode before you perform any other configuration because changing the firewall mode clears the running configuration.

Prerequisites

When you change modes, the ASA clears the running configuration (see Guidelines for Firewall Mode, page 5-7 for more information).

- If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration. See Backing Up and Restoring Configurations or Other Files, page 36-26.
- Use the CLI at the console port to change the mode. If you use any other type of session, including the ASDM Command Line Interface tool or SSH, you will be disconnected when the configuration is cleared, and you will have to reconnect to the ASA using the console port in any case.
- Set the mode within the context.

Procedure

To set the firewall mode to transparent and also configure ASDM management access after the configuration is cleared, see Configure ASDM Access, page 2-6.

Step 1

Set the firewall mode to transparent:

```
firwwall transparent
```  

Example:

```
ciscoasa(config)# firewall transparent
```  

To change the mode to routed, enter the no firewall transparent command.

---

### Table 5-1  Unsupported Features in Transparent Mode

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN termination for through traffic</td>
<td>The transparent firewall supports site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the ASA. You can pass VPN traffic through the ASA using an extended ACL, but it does not terminate non-management connections. Clientless SSL VPN is also not supported.</td>
</tr>
<tr>
<td>Unified Communications</td>
<td>—</td>
</tr>
</tbody>
</table>
Configure ARP Inspection for the Transparent Firewall

To configure ARP Inspection, perform the following steps:

**Step 1** Add static ARP entries according to Add a Static ARP Entry, page 5-10. ARP inspection compares ARP packets with static ARP entries in the ARP table, so static ARP entries are required for this feature.

**Step 2** Enable ARP inspection according to Enable ARP Inspection, page 5-11.

Add a Static ARP Entry

ARP inspection compares ARP packets with static ARP entries in the ARP table. Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

Note

The transparent firewall uses dynamic ARP entries in the ARP table for traffic to and from the ASA, such as management traffic.

Procedure

**Step 1** Add a static ARP entry:

```
arp interface_name ip_address mac_address
```

Example:

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

This allows ARP responses from the router at 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface.
Enable ARP Inspection

This section describes how to enable ARP inspection.

Procedure

Step 1
Enable ARP inspection:
arp-inspection interface_name enable [flood | no-flood]

Example:
ciscoasa(config)# arp-inspection outside enable no-flood

The flood keyword forwards non-matching ARP packets out all interfaces, and no-flood drops non-matching packets.

The default setting is to flood non-matching packets. To restrict ARP through the ASA to only static entries, then set this command to no-flood.

Customize the MAC Address Table for the Transparent Firewall

This section describes how you can customize the MAC address table.

- Add a Static MAC Address, page 5-11
- Set the MAC Address Timeout, page 5-12
- Disable MAC Address Learning, page 5-12

Add a Static MAC Address

Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the ASA drops the traffic and generates a system message. When you add a static ARP entry (see Add a Static ARP Entry, page 5-10), a static MAC address entry is automatically added to the MAC address table.

To add a static MAC address to the MAC address table, perform the following steps.

Procedure

Step 1
Add a static MAC address entry:
mac-address-table static interface_name mac_address

Example:
Customize the MAC Address Table for the Transparent Firewall

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

The *interface_name* is the source interface.

---

Set the MAC Address Timeout

The default timeout value for dynamic MAC address table entries is 5 minutes, but you can change the timeout. To change the timeout, perform the following steps.

**Procedure**

**Step 1**
Set the MAC address entry timeout:
```
mac-address-table aging-time timeout_value
```

Example:
```
ciscoasa(config)# mac-address-table aging-time 10
```

The *timeout_value* (in minutes) is between 5 and 720 (12 hours). 5 minutes is the default.

---

Disable MAC Address Learning

By default, each interface automatically learns the MAC addresses of entering traffic, and the ASA adds corresponding entries to the MAC address table. You can disable MAC address learning if desired, however, unless you statically add MAC addresses to the table, no traffic can pass through the ASA.

To disable MAC address learning, perform the following steps:

**Procedure**

**Step 1**
Disable MAC address learning:
```
mac-learn interface_name disable
```

Example:
```
ciscoasa(config)# mac-learn inside disable
```

The *no* form of this command reenables MAC address learning. The *clear configure mac-learn* command reenables MAC address learning on all interfaces.
Monitoring the Transparent Firewall

### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp-inspection</td>
<td>Monitors ARP Inspection. Shows the current settings for ARP inspection on all interfaces.</td>
</tr>
<tr>
<td>show mac-address-table [interface_name]</td>
<td>Monitors the MAC address table. You can view the entire MAC address table (including static and dynamic entries for both interfaces), or you can view the MAC address table for an interface.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show mac-address-table` command that shows the entire table:

```
ciscoasa# show mac-address-table
interface   mac address     type    Time Left
outside   0009.7cbe.2100      static   -
inside     0010.7cbe.6101     static   -
inside     0009.7cbe.5101     dynamic  10
```

The following is sample output from the `show mac-address-table` command that shows the table for the inside interface:

```
ciscoasa# show mac-address-table inside
interface   mac address     type    Time Left
inside     0010.7cbe.6101     static   -
inside     0009.7cbe.5101     dynamic  10
```

### Examples for Firewall Mode

This section includes examples of how traffic moves through the ASA.

- How Data Moves Through the ASA in Routed Firewall Mode, page 5-13
- How Data Moves Through the Transparent Firewall, page 5-19

### How Data Moves Through the ASA in Routed Firewall Mode

This section describes how data moves through the ASA in routed firewall mode.

- An Inside User Visits a Web Server, page 5-14
- An Outside User Visits a Web Server on the DMZ, page 5-15
- An Inside User Visits a Web Server on the DMZ, page 5-16
- An Outside User Attempts to Access an Inside Host, page 5-16
- A DMZ User Attempts to Access an Inside Host, page 5-18
An Inside User Visits a Web Server

Figure 5-3 shows an inside user accessing an outside web server.

Figure 5-3  Inside to Outside

The following steps describe how data moves through the ASA (see Figure 5-3):

1. The user on the inside network requests a web page from www.example.com.

2. The ASA receives the packet and because it is a new session, the ASA verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
   For multiple context mode, the ASA first classifies the packet to a context.

3. The ASA translates the local source address (10.1.2.27) to the global address 209.165.201.10, which is on the outside interface subnet.
   The global address could be on any subnet, but routing is simplified when it is on the outside interface subnet.

4. The ASA then records that a session is established and forwards the packet from the outside interface.

5. When www.example.com responds to the request, the packet goes through the ASA, and because the session is already established, the packet bypasses the many lookups associated with a new connection. The ASA performs NAT by untranslating the global destination address to the local user address, 10.1.2.27.

6. The ASA forwards the packet to the inside user.
An Outside User Visits a Web Server on the DMZ

Figure 5-4 shows an outside user accessing the DMZ web server.

Figure 5-4    Outside to DMZ

The following steps describe how data moves through the ASA (see Figure 5-4):

1. A user on the outside network requests a web page from the DMZ web server using the global destination address of 209.165.201.3, which is on the outside interface subnet.

2. The ASA receives the packet and untranslates the destination address to the local address 10.1.1.3.

3. Because it is a new session, the ASA verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
   For multiple context mode, the ASA first classifies the packet to a context.

4. The ASA then adds a session entry to the fast path and forwards the packet from the DMZ interface.

5. When the DMZ web server responds to the request, the packet goes through the ASA and because the session is already established, the packet bypasses the many lookups associated with a new connection. The ASA performs NAT by translating the local source address to 209.165.201.3.

6. The ASA forwards the packet to the outside user.
An Inside User Visits a Web Server on the DMZ

Figure 5-5 shows an inside user accessing the DMZ web server.

Figure 5-5  Inside to DMZ

The following steps describe how data moves through the ASA (see Figure 5-5):
1. A user on the inside network requests a web page from the DMZ web server using the destination address of 10.1.1.3.
2. The ASA receives the packet and because it is a new session, the ASA verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
   For multiple context mode, the ASA first classifies the packet to a context.
3. The ASA then records that a session is established and forwards the packet out of the DMZ interface.
4. When the DMZ web server responds to the request, the packet goes through the fast path, which lets the packet bypass the many lookups associated with a new connection.
5. The ASA forwards the packet to the inside user.

An Outside User Attempts to Access an Inside Host

Figure 5-6 shows an outside user attempting to access the inside network.
The following steps describe how data moves through the ASA (see Figure 5-6):

1. A user on the outside network attempts to reach an inside host (assuming the host has a routable IP address).

   If the inside network uses private addresses, no outside user can reach the inside network without NAT. The outside user might attempt to reach an inside user by using an existing NAT session.

2. The ASA receives the packet and because it is a new session, the ASA verifies if the packet is allowed according to the security policy (access lists, filters, AAA).

3. The packet is denied, and the ASA drops the packet and logs the connection attempt.

   If the outside user is attempting to attack the inside network, the ASA employs many technologies to determine if a packet is valid for an already established session.
A DMZ User Attempts to Access an Inside Host

Figure 5-7 shows a user in the DMZ attempting to access the inside network.

The following steps describe how data moves through the ASA (see Figure 5-7):

1. A user on the DMZ network attempts to reach an inside host. Because the DMZ does not have to route the traffic on the Internet, the private addressing scheme does not prevent routing.

2. The ASA receives the packet and because it is a new session, the ASA verifies if the packet is allowed according to the security policy (access lists, filters, AAA).

   The packet is denied, and the ASA drops the packet and logs the connection attempt.
How Data Moves Through the Transparent Firewall

Figure 5-8 shows a typical transparent firewall implementation with an inside network that contains a public web server. The ASA has an access list so that the inside users can access Internet resources. Another access list lets the outside users access only the web server on the inside network.

This section describes how data moves through the ASA.

- An Inside User Visits a Web Server, page 5-20
- An Inside User Visits a Web Server Using NAT, page 5-21
- An Outside User Attempts to Access an Inside Host, page 5-23
An Inside User Visits a Web Server

Figure 5-9 shows an inside user accessing an outside web server.

The following steps describe how data moves through the ASA (see Figure 5-9):

1. The user on the inside network requests a web page from www.example.com.

2. The ASA receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

   For multiple context mode, the ASA first classifies the packet to a context.

3. The ASA records that a session is established.

4. If the destination MAC address is in its table, the ASA forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 209.165.201.2.

   If the destination MAC address is not in the ASA table, the ASA attempts to discover the MAC address by sending an ARP request or a ping. The first packet is dropped.

5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.

6. The ASA forwards the packet to the inside user.
An Inside User Visits a Web Server Using NAT

Figure 5-10 shows an inside user accessing an outside web server.

The following steps describe how data moves through the ASA (see Figure 5-10):

1. The user on the inside network requests a web page from www.example.com.
2. The ASA receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
   
   For multiple context mode, the ASA first classifies the packet according to a unique interface.
3. The ASA translates the real address (10.1.2.27) to the mapped address 209.165.201.10.
   
   Because the mapped address is not on the same network as the outside interface, then be sure the upstream router has a static route to the mapped network that points to the ASA.
4. The ASA then records that a session is established and forwards the packet from the outside interface.
5. If the destination MAC address is in its table, the ASA forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 10.1.2.1.
   
   If the destination MAC address is not in the ASA table, the ASA attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.
6. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.
7. The ASA performs NAT by untranslating the mapped address to the real address, 10.1.2.27.
An Outside User Visits a Web Server on the Inside Network

Figure 5-11 shows an outside user accessing the inside web server.

The following steps describe how data moves through the ASA (see Figure 5-11):

1. A user on the outside network requests a web page from the inside web server.

2. The ASA receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
   
   For multiple context mode, the ASA first classifies the packet to a context.

3. The ASA records that a session is established.

4. If the destination MAC address is in its table, the ASA forwards the packet out of the inside interface. The destination MAC address is that of the downstream router, 209.165.201.1.
   
   If the destination MAC address is not in the ASA table, the ASA attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.

5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.

6. The ASA forwards the packet to the outside user.
An Outside User Attempts to Access an Inside Host

Figure 5-12 shows an outside user attempting to access a host on the inside network.

The following steps describe how data moves through the ASA (see Figure 5-12):

1. A user on the outside network attempts to reach an inside host.
2. The ASA receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies if the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
   For multiple context mode, the ASA first classifies the packet to a context.
3. The packet is denied because there is no access list permitting the outside host, and the ASA drops the packet.
4. If the outside user is attempting to attack the inside network, the ASA employs many technologies to determine if a packet is valid for an already established session.
## History for the Firewall Mode

### Table 5-2  Feature History for Firewall Mode

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Transparent Firewall Mode     | 7.0(1)            | A transparent firewall is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.  
                                |                   | We introduced the following commands: **firewall transparent**, **show firewall**.                                                                     |
| ARP inspection                | 7.0(1)            | ARP inspection compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table.                      
                                |                   | We introduced the following commands: **arp**, **arp-inspection**, and **show arp-inspection**.                                                          |
| MAC address table             | 7.0(1)            | Transparent firewall mode uses a MAC address table.                                                                                                                                                           
                                |                   | We introduced the following commands: **mac-address-table static**, **mac-address-table aging-time**, **mac-learn disable**, and **show mac-address-table**. |
| Transparent firewall bridge groups | 8.4(1)            | 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.  
                                |                   | **Note** 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.                                                                                                                                                      
                                |                   | We introduced the following commands: **interface bvi**, **bridge-group**, **show bridge-group**.                                                                                                              |
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`.

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.

We modified the following command: `firewall transparent`.

The bridge group maximum was increased from 8 to 250 bridge groups. You can configure up to 250 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group.

We modified the following commands: `interface bvi bridge-group`.
Chapter 5  Transparent or Routed Firewall Mode

History for the Firewall Mode
PART 2

High Availability and Scalability
Multiple Context Mode

This chapter describes how to configure multiple security contexts on the Cisco ASA.

- About Security Contexts, page 6-1
- Licensing for Multiple Context Mode, page 6-13
- Guidelines for Multiple Context Mode, page 6-14
- Defaults for Multiple Context Mode, page 6-14
- Configure Multiple Contexts, page 6-14
- Change Between Contexts and the System Execution Space, page 6-23
- Manage Security Contexts, page 6-24
- Monitoring Security Contexts, page 6-28
- Examples for Multiple Context Mode, page 6-38
- History for Multiple Context Mode, page 6-39

About Security Contexts

You can partition a single ASA into multiple virtual devices, known as security contexts. Each context acts as an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. For unsupported features in multiple context mode, see Guidelines for Multiple Context Mode, page 6-14.

This section provides an overview of security contexts.

- Common Uses for Security Contexts, page 6-2
- Context Configuration Files, page 6-2
- How the ASA Classifies Packets, page 6-3
- Cascading Security Contexts, page 6-6
- Management Access to Security Contexts, page 6-7
- About Resource Management, page 6-8
- About MAC Addresses, page 6-11
Common Uses for Security Contexts

You might want to use multiple security contexts in the following situations:

- You are a service provider and want to sell security services to many customers. By enabling multiple security contexts on the ASA, you can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.
- You are a large enterprise or a college campus and want to keep departments completely separate.
- You are an enterprise that wants to provide distinct security policies to different departments.
- You have any network that requires more than one ASA.

Context Configuration Files

This section describes how the ASA implements multiple context mode configurations.

- Context Configurations, page 6-2
- System Configuration, page 6-2
- Admin Context Configuration, page 6-2

Context Configurations

For each context, the ASA includes a configuration that identifies the security policy, interfaces, and all the options you can configure on a standalone device. You can store context configurations in flash memory, or you can download them from a TFTP, FTP, or HTTP(S) server.

System Configuration

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and other context operating parameters 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 system configuration does include a specialized failover interface for failover traffic only.

Admin Context Configuration

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users. The admin context must reside on flash memory, and not remotely.

If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal flash memory called admin.cfg. This context is named “admin.” If you do not want to use admin.cfg as the admin context, you can change the admin context.
How the ASA Classifies Packets

Each packet that enters the ASA must be classified, so that the ASA can determine to which context to send a packet.

- Valid Classifier Criteria, page 6-3
- Classification Examples, page 6-4

**Note**

If the destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each context.

Valid Classifier Criteria

This section describes the criteria used by the classifier.

- Unique Interfaces, page 6-3
- Unique MAC Addresses, page 6-3
- NAT Configuration, page 6-3

**Note**

For management traffic destined for an interface, the interface IP address is used for classification.

The routing table is not used for packet classification.

Unique Interfaces

If only one context is associated with the ingress interface, the ASA classifies the packet into that context. In transparent firewall mode, unique interfaces for contexts are required, so this method is used to classify packets at all times.

Unique MAC Addresses

If multiple contexts share an interface, then the classifier uses unique MAC addresses assigned to the interface in each context. An upstream router cannot route directly to a context without unique MAC addresses. By default, auto-generation of MAC addresses is enabled. You can also set the MAC addresses manually when you configure each interface.

NAT Configuration

If you disable use of unique MAC addresses, then the ASA uses the mapped addresses in your NAT configuration to classify packets. We recommend using MAC addresses instead of NAT, so that traffic classification can occur regardless of the completeness of the NAT configuration.
Classification Examples

Figure 6-1 shows multiple contexts sharing an outside interface. The classifier assigns the packet to Context B because Context B includes the MAC address to which the router sends the packet.

Figure 6-1  Packet Classification with a Shared Interface Using MAC Addresses
Note that all new incoming traffic must be classified, even from inside networks. Figure 6-2 shows a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is Gigabit Ethernet 0/1.3, which is assigned to Context B.

*Figure 6-2    Incoming Traffic from Inside Networks*
For transparent firewalls, you must use unique interfaces. Figure 6-3 shows a packet destined to a host on the Context B inside network from the Internet. The classifier assigns the packet to Context B because the ingress interface is Gigabit Ethernet 1/0.3, which is assigned to Context B.

**Figure 6-3  Transparent Firewall Contexts**

**Cascading Security Contexts**

Placing a context directly in front of another context is called *cascading contexts*; the outside interface of one context is the same interface as the inside interface of another context. You might want to cascade contexts if you want to simplify the configuration of some contexts by configuring shared parameters in the top context.

---

**Note**

Cascading contexts requires unique MAC addresses for each context interface (the default setting). Because of the limitations of classifying packets on shared interfaces without MAC addresses, we do not recommend using cascading contexts without unique MAC addresses.
Figure 6-4 shows a gateway context with two contexts behind the gateway.

**Figure 6-4 Cascading Contexts**

Management Access to Security Contexts

The ASA provides system administrator access in multiple context mode as well as access for individual context administrators. The following sections describe logging in as a system administrator or as a context administrator:

- System Administrator Access, page 6-7
- Context Administrator Access, page 6-8

System Administrator Access

You can access the ASA as a system administrator in two ways:

- Access the ASA console.
  
  From the console, you access the system execution space, which means that any commands you enter affect only the system configuration or the running of the system (for run-time commands).

- Access the admin context using Telnet, SSH, or ASDM.
  
  See Chapter 35, “Management Access,” to enable Telnet, SSH, and ASDM access.

As the system administrator, you can access all contexts.

When you change to a context from admin or the system, your username changes to the default “enable_15” username. If you configured command authorization in that context, you need to either configure authorization privileges for the “enable_15” user, or you can log in as a different name for which you provide sufficient privileges. To log in with a new username, enter the `login` command.
example, you log in to the admin context with the username “admin.” The admin context does not have any command authorization configuration, but all other contexts include command authorization. For convenience, each context configuration includes a user “admin” with maximum privileges. When you change from the admin context to context A, your username is altered to enable_15, so you must log in again as “admin” by entering the `login` command. When you change to context B, you must again enter the `login` command to log in as “admin.”

The system execution space does not support any AAA commands, but you can configure its own enable password, as well as usernames in the local database to provide individual logins.

**Context Administrator Access**

You can access a context using Telnet, SSH, or ASDM. If you log in to a non-admin context, you can only access the configuration for that context. You can provide individual logins to the context. See Chapter 35, “Management Access,” to enable Telnet, SSH, and ASDM access and to configure management authentication.

**About Resource Management**

By default, all security contexts have unlimited access to the resources of the ASA, except where maximum limits per context are enforced; the only exception is VPN resources, which are disabled by default. 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. For VPN resources, you must configure resource management to allow any VPN tunnels.

- Resource Classes, page 6-8
- Resource Limits, page 6-8
- Default Class, page 6-9
- Use Oversubscribed Resources, page 6-10
- Use Unlimited Resources, page 6-11

**Resource Classes**

The ASA manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class. To use the settings of a class, assign the context to the class when you define the context. All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to default. You can only assign a context to one resource class. The exception to this rule is that limits that are undefined in the member class are inherited from the default class; so in effect, a context could be a member of default plus another class.

**Resource Limits**

You can set the limit for individual resources as a percentage (if there is a hard system limit) or as an absolute value.

For most resources, the ASA does not set aside a portion of the resources for each context assigned to the class; rather, the ASA sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can “use up” those resources, potentially affecting service
to other contexts. The exception is VPN resource types, which you cannot oversubscribe, so the resources assigned to each context are guaranteed. To accommodate temporary bursts of VPN sessions beyond the amount assigned, the ASA supports a “burst” VPN resource type, which is equal to the remaining unassigned VPN sessions. The burst sessions can be oversubscribed, and are available to contexts on a first-come, first-served basis.

**Default Class**

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a 2 percent limit for all concurrent connections, but no other limits, then all other limits are inherited from the default class. Conversely, if you create a class with a limit for all resources, the class uses no settings from the default class.

For most resources, the default class provides unlimited access to resources for all contexts, except for the following limits:

- Telnet sessions—5 sessions. (The maximum per context.)
- SSH sessions—5 sessions. (The maximum per context.)
- IPsec sessions—5 sessions. (The maximum per context.)
- MAC addresses—65,535 entries. (The maximum per context.)
- VPN site-to-site tunnels—0 sessions. (You must manually configure the class to allow any VPN sessions.)
Figure 6-5 shows the relationship between the default class and other classes. Contexts A and C belong to classes with some limits set; other limits are inherited from the default class. Context B inherits no limits from default because all limits are set in its class, the Gold class. Context D was not assigned to a class, and is by default a member of the default class.

Use Oversubscribed Resources

You can oversubscribe the ASA by assigning more than 100 percent of a resource across all contexts (with the exception of non-burst VPN resources). For example, you can set the Bronze class to limit connections to 20 percent per context, and then assign 10 contexts to the class for a total of 200 percent. If contexts concurrently use more than the system limit, then each context gets less than the 20 percent you intended. (See Figure 6-6.)
Use Unlimited Resources

The ASA lets you assign unlimited access to one or more resources in a class, instead of a percentage or absolute number. When a resource is unlimited, contexts can use as much of the resource as the system has available. For example, Context A, B, and C are in the Silver Class, which limits each class member to 1 percent of the connections, for a total of 3 percent; but the three contexts are currently only using 2 percent combined. Gold Class has unlimited access to connections. The contexts in the Gold Class can use more than the 97 percent of “unassigned” connections; they can also use the 1 percent of connections not currently in use by Context A, B, and C, even if that means that Context A, B, and C are unable to reach their 3 percent combined limit. (See Figure 6-7.) Setting unlimited access is similar to oversubscribing the ASA, except that you have less control over how much you oversubscribe the system.

Figure 6-7 Unlimited Resources

About MAC Addresses

To allow contexts to share interfaces, the ASA assigns virtual MAC addresses to each shared context interface by default. To customize or disable auto-generation, see Assign MAC Addresses to Context Interfaces Automatically, page 6-23.

The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then other classification methods are attempted that might not provide full coverage. See How the ASA Classifies Packets, page 6-3 for information about classifying packets.

In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See Configuring the MAC Address, MTU, and TCP MSS, page 11-9 to manually set the MAC address.

- Default MAC Address, page 6-12
- Interaction with Manual MAC Addresses, page 6-12
- Failover MAC Addresses, page 6-12
- MAC Address Format, page 6-12
Default MAC Address

Automatic MAC address generation is enabled by default. The ASA autogenerates the prefix based on the last two bytes of the interface (ASA 5500-X) or backplane (ASASM) MAC address. You can customize the prefix if desired.

If you disable MAC address generation, see the following default MAC addresses:

- For the ASA 5500-X series appliances—The physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.
- For the ASASM—All VLAN interfaces use the same MAC address, derived from the backplane MAC address.

See also MAC Address Format, page 6-12.

Note

(8.5(1.6) and earlier) To maintain hitless upgrade for failover pairs, the ASA does not convert an existing legacy auto-generation 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, especially for the ASASM. 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, reenable MAC address autogeneration to use a prefix. For more information about the legacy method, see the `mac-address auto` command in the command reference.

Interaction with Manual MAC Addresses

If you manually assign a MAC address and also enable auto-generation, then the manually assigned MAC address is used. If you later remove the manual MAC address, the auto-generated address is used.

Because auto-generated addresses (when using a prefix) start with A2, you cannot start manual MAC addresses with A2 if you also want to use auto-generation.

Failover MAC Addresses

For use with failover, the ASA generates both an active and standby MAC address for each interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption. See MAC Address Format, page 6-12 section for more information.

MAC Address Format

The ASA generates the MAC address using the following format:

A2xx.yyyzz.zzzz

Where xx.yy is a user-defined prefix or an autogenerated prefix based on the last two bytes of the interface (ASA 5500-X) or backplane (ASASM) MAC address, and zz.zzzz is an internal counter generated by the ASA. For the standby MAC address, the address is identical except that the internal counter is increased by 1.

For an example of how the prefix is used, if you set a prefix of 77, then the ASA converts 77 into the hexadecimal value 004D (yyxx). When used in the MAC address, the prefix is reversed (xxyy) to match the ASA native form:
A24D.00zz.zzzz
For a prefix of 1009 (03F1), the MAC address is:
A2F1.03zz.zzzz

Note
The MAC address format without a prefix is a legacy version not supported on newer ASA versions. See the `mac-address auto` command in the command reference for more information about the legacy format.

## Licensing for Multiple Context Mode

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>No support.</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>• Base License: No support.</td>
</tr>
<tr>
<td></td>
<td>• Security Plus License: 2 contexts.</td>
</tr>
<tr>
<td></td>
<td><code>Optional license: 5 contexts.</code></td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>Base License: 2 contexts.</td>
</tr>
<tr>
<td></td>
<td><code>Optional license: 5 contexts.</code></td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>Base License: 2 contexts.</td>
</tr>
<tr>
<td></td>
<td><code>Optional licenses: 5, 10, or 20 contexts.</code></td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>Base License: 2 contexts.</td>
</tr>
<tr>
<td></td>
<td><code>Optional licenses: 5, 10, 20, or 50 contexts.</code></td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td>Base License: 2 contexts.</td>
</tr>
<tr>
<td></td>
<td><code>Optional licenses: 5, 10, 20, 50, or 100 contexts.</code></td>
</tr>
<tr>
<td>ASA 5585-X with</td>
<td>Base License: 2 contexts.</td>
</tr>
<tr>
<td>SSP-10</td>
<td><code>Optional licenses: 5, 10, 20, 50, or 100 contexts.</code></td>
</tr>
<tr>
<td>ASA 5585-X with</td>
<td>Base License: 2 contexts.</td>
</tr>
<tr>
<td>SSP-20, -40, and -60</td>
<td><code>Optional licenses: 5, 10, 20, 50, 100, or 250 contexts.</code></td>
</tr>
<tr>
<td>ASASM</td>
<td>Base License: 2 contexts.</td>
</tr>
<tr>
<td></td>
<td><code>Optional licenses: 5, 10, 20, 50, 100, or 250 contexts.</code></td>
</tr>
<tr>
<td>ASA v</td>
<td>No support.</td>
</tr>
</tbody>
</table>

## Prerequisites

After you are in multiple context mode, connect to the system or the admin context to access the system configuration. You cannot configure the system from a non-admin context. By default, after you enable multiple context mode, you can connect to the admin context by using the default management IP address. See Chapter 2, “Getting Started,” for more information about connecting to the ASA.
Guidelines for Multiple Context Mode

Failover Guidelines
Active/Active mode failover is only supported in multiple context mode.

IPv6 Guidelines
Supports IPv6.

Note
Cross context IPv6 routing is not supported.

Unsupported Features
Multiple context mode does not support the following features:
- RIP
- OSPFv3. (OSPFv2 is supported.)
- Multicast routing
- Threat Detection
- Unified Communications
- QoS
- Remote access VPN. (Site-to-site VPN is supported.)

Additional Guidelines
- The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match.
- If you store context configurations in the root directory of flash memory, on some models you might run out of room in that directory, even though there is available memory. In this case, create a subdirectory for your configuration files. Background: some models, such as the ASA 5585-X, use the FAT 16 file system for internal flash memory, and if you do not use 8.3-compliant short names, or use uppercase characters, then fewer than 512 files and folders can be stored because the file system uses up slots to store long file names (see http://support.microsoft.com/kb/120138/en-us).

Defaults for Multiple Context Mode
- By default, the ASA is in single context mode.
- See Default Class, page 6-9.
- See Default MAC Address, page 6-12.

Configure Multiple Contexts
To configure multiple context mode, perform the following steps:

Step 1
Enable multiple context mode. See Enable or Disable Multiple Context Mode, page 6-15.
Configure Multiple Contexts

Step 2  (Optional) Configure classes for resource management. See Configure a Class for Resource Management, page 6-16. Note: For VPN support, you must configure VPN resources in a resource class; the default class does not allow VPN.

Step 3  Configure interfaces in the system execution space.
- ASA 5500-X—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
- ASASM—ASASM quick start guide.


Step 5  (Optional) Customize MAC address assignments. See Assign MAC Addresses to Context Interfaces Automatically, page 6-23.

Step 6  Complete interface configuration in the context. See Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”

Enable or Disable Multiple Context Mode

Your ASA might already be configured for multiple security contexts depending on how you ordered it from Cisco. If you need to convert from single mode to multiple mode, follow the procedures in this section.

- Enable Multiple Context Mode, page 6-15
- Restore Single Context Mode, page 6-16

Enable Multiple Context Mode

When you convert from single mode to multiple mode, the ASA converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal flash memory). The original running configuration is saved as old_running.cfg (in the root directory of the internal flash memory). The original startup configuration is not saved. The ASA automatically adds an entry for the admin context to the system configuration with the name “admin.”

Prerequisites

Back up your startup configuration. When you convert from single mode to multiple mode, the ASA converts the running configuration into two files. The original startup configuration is not saved. See Backing Up and Restoring Configurations or Other Files, page 36-26.

Procedure

Step 1  Change to multiple context mode:

```
mode multiple
```

Example:

```
ciscoasa(config)# mode multiple
```
You are prompted to reboot the ASA.

**Restore Single Context Mode**

To copy the old running configuration to the startup configuration and to change the mode to single mode, perform the following steps.

**Before You Begin**
Perform this procedure in the system execution space.

**Procedure**

**Step 1** Copy the backup version of your original running configuration to the current startup configuration:

```plaintext
copy disk0:old_running.cfg startup-config
```

Example:

```plaintext
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

**Step 2** Set the mode to single mode:

```plaintext
mode single
```

Example:

```plaintext
ciscoasa(config)# mode single
```

You are prompted to reboot the ASA.

**Configure a Class for Resource Management**

To configure a class in the system configuration, perform the following steps. You can change the value of a particular resource limit by reentering the command with a new value.

**Before You Begin**
Perform this procedure in the system execution space.

**Guidelines**

Table 6-1 lists the resource types and the limits. See also the `show resource types` command.
### Table 6-1 Resource Names and Limits

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Rate or Concurrent</th>
<th>Minimum and Maximum Number per Context</th>
<th>System Limit¹</th>
<th>Description</th>
</tr>
</thead>
</table>
| asdm          | Concurrent         | 1 minimum 5 maximum                    | 32             | ASDM management sessions.  
Note: ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 32 ASDM sessions represents a limit of 64 HTTPS sessions. |
| conns²        | Concurrent or Rate  | N/A                                    | N/A            | TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.  
Note: See Supported Feature Licenses Per Model, page 3-1 for the connection limit available for your model. |
| hosts         | Concurrent         | N/A                                    | N/A            | Hosts that can connect through the ASA. |
| inspects      | Rate               | N/A                                    | N/A            | Application inspections per second. |
| mac-addresses | Concurrent         | N/A                                    | 65,535         | For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. |
| routes        | Concurrent         | N/A                                    | N/A            | Dynamic routes. |
| vpn burst other| Concurrent         | N/A                                    | N/A            | The number of site-to-site VPN sessions allowed beyond the amount assigned to a context with vpn other. For example, if your model supports 5000 sessions, and you assign 4000 sessions across all contexts with vpn other, then the remaining 1000 sessions are available for vpn burst other. Unlike vpn other, which guarantees the sessions to the context, vpn burst other can be oversubscribed; the burst pool is available to all contexts on a first-come, first-served basis. |
| vpn other     | Concurrent         | N/A                                    | See Supported Feature Licenses Per Model, page 3-1 for the Other VPN sessions available for your model. | Site-to-site VPN sessions. You cannot oversubscribe this resource; all context assignments combined cannot exceed the model limit. The sessions you assign for this resource are guaranteed to the context. |
| ssh           | Concurrent         | 1 minimum 5 maximum                    | 100            | SSH sessions. |
| syslogs       | Rate               | N/A                                    | N/A            | Syslog messages per second. |
Configure Multiple Contexts

Chapter 6      Multiple Context Mode

Configure Multiple Contexts

**Procedure**

**Step 1**

Specify the class name and enter the class configuration mode:

```
class name
```

Example:

```
ciscoasa(config)# class gold
```

The name is a string up to 20 characters long. To set the limits for the default class, enter `default` for the name.

**Step 2**

Set the resource limit for a resource type:

```
limit-resource [rate] resource_name number[%]
```

Example:

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- See Table 6-1 for a list of resource types. If you specify `all`, then all resources are configured with the same value. If you also specify a value for a particular resource, the limit overrides the limit set for `all`
- Enter the `rate` argument to set the rate per second for certain resources.
- For most resources, specify `0` for the `number` to set the resource to be unlimited or to be the system limit, if available. For VPN resources, `0` sets the limit to none.
- For resources that do not have a system limit, you cannot set the percentage (`%`); you can only set an absolute value.

**Examples**

For example, to set the default class limit for conns to 10 percent instead of unlimited, and to allow 5 site-to-site VPN tunnels with 2 tunnels allowed for VPN burst, enter the following commands:

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

### Table 6-1 Resource Names and Limits (continued)

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Rate or Concurrent</th>
<th>Minimum and Maximum Number per Context</th>
<th>System Limit1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>telnet</td>
<td>Concurrent</td>
<td>1 minimum</td>
<td>100</td>
<td>Telnet sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xlates2</td>
<td>Concurrent</td>
<td>N/A</td>
<td>N/A</td>
<td>Network address translations.</td>
</tr>
</tbody>
</table>

1. If this column value is N/A, then you cannot set a percentage of the resource because there is no hard system limit for the resource.

2. Syslog messages are generated for whichever limit is lower xlates or conns. For example, if you set the xlates limit to 7 and the conns to 9, then the ASA only generates syslog message 321001 (“Resource ‘xlates’ limit of 7 reached for context ‘ctx1’”) and not 321002 (“Resource ‘conn rate’ limit of 5 reached for context ‘ctx1’”).
All other resources remain at unlimited.

To add a class called gold, enter the following commands:

```bash
ciscoasa(config)# class gold
```
```bash
ciscoasa(config-class)# limit-resource mac-addresses 10000
```
```bash
ciscoasa(config-class)# limit-resource conns 15%
```
```bash
ciscoasa(config-class)# limit-resource rate conns 1000
```
```bash
ciscoasa(config-class)# limit-resource rate inspects 500
```
```bash
ciscoasa(config-class)# limit-resource hosts 9000
```
```bash
ciscoasa(config-class)# limit-resource asdm 5
```
```bash
ciscoasa(config-class)# limit-resource ssh 5
```
```bash
ciscoasa(config-class)# limit-resource rate syslogs 5000
```
```bash
ciscoasa(config-class)# limit-resource telnet 5
```
```bash
ciscoasa(config-class)# limit-resource xlates 36000
```
```bash
ciscoasa(config-class)# limit-resource routes 5000
```
```bash
ciscoasa(config-class)# limit-resource vpn other 10
```
```bash
ciscoasa(config-class)# limit-resource vpn burst other 5
```

## Configure a Security Context

The security context definition in the system configuration identifies the context name, configuration file URL, interfaces that a context can use, and other settings.

### Before You Begin

- Perform this procedure in the system execution space.
- For the ASASM, assign VLANs to the ASASM on the switch according to the ASASM quick start guide.
- For the ASA 5500-X, configure physical interface parameters, VLAN subinterfaces, EtherChannels, and redundant interfaces according to Chapter 9, “Basic Interface Configuration (ASA Appliances).”
- If you do not have an admin context (for example, if you clear the configuration) then you must first specify the admin context name by entering the following command:

```bash
ciscoasa(config)# admin-context name
```

Although this context does not exist yet in your configuration, you can subsequently enter the `context name` command to continue the admin context configuration.

### Procedure

#### Step 1

Add or modify a context:

```bash
context name
```

Example:

```bash
ciscoasa(config)# context administrator
```

The name is a string up to 32 characters long. This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen.
Configure Multiple Contexts

**Note**
“System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.

**Step 2** (Optional) Add a description for this context:

```plaintext
description text
```

Example:
```
ciscoasa(config-ctx)# description Administrator Context
```

**Step 3** Specify the interfaces you can use in the context:

To allocate an interface:

```plaintext
allocate-interface interface_id [mapped_name] [visible | invisible]
```

To allocate one or more subinterfaces:

```plaintext
allocate-interface interface_id.subinterface[-interface_id.subinterface] [mapped_name[-mapped_name]] [visible | invisible]
```

Example:
```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305 int3-int8
```

**Note** Do not include a space between the interface type and the port number.

- Enter these commands multiple times to specify different ranges. If you remove an allocation with the `no` form of this command, then any context commands that include this interface are removed from the running configuration.
- Transparent firewall mode allows a limited number of interfaces to pass through traffic; however, you can use a dedicated management interface, Management slot/port (physical, subinterface, redundant, or EtherChannel), as an additional interface for management traffic. A separate management interface is not available for the ASASM.
- You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.
- The `mapped_name` is an alphanumeric alias for the interface that can be used within the context instead of the interface ID. If you do not specify a mapped name, the interface ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces the context is using. A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names: `int0`, `inta`, `int_0`
- If you specify a range of subinterfaces, you can specify a matching range of mapped names. Follow these guidelines for ranges:
  - The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range: `int0-int10`. If you enter `gig0/1.1-gig0/1.5 happy1-sads`, for example, the command fails.
The numeric portion of the mapped name must include the same quantity of numbers as the subinterface range. For example, both ranges include 100 interfaces: `gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100`. If you enter `gig0/0.100-gig0/0.199 int1-int15`, for example, the command fails.

- Specify `visible` to see the real interface ID in the `show interface` command if you set a mapped name. The default `invisible` keyword shows only the mapped name.

**Step 4**

Identify the URL from which the system downloads the context configuration:

```
config-url url
```

Example:

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

**Step 5**

(Optional) Assign the context to a resource class:

If you do not specify a class, the context belongs to the default class. You can only assign a context to one resource class.

```
member class_name
```

Example:

```
ciscoasa(config-ctx)# member gold
```

**Step 6**

(Optional) Assign an IPS virtual sensor to this context if you have the IPS module installed:

```
allocate-ips sensor_name [mapped_name] [default]
```

Example:

```
ciscoasa(config-ctx)# allocate-ips sensor1 highsec
```

See the firewall configuration guide for detailed information about virtual sensors.

- When you add a context URL, the system immediately loads the context so that it is running, if the configuration is available.

- Enter the `allocate-interface` command(s) before you enter the `config-url` command. If you enter the `config-url` command first, the ASA loads the context configuration immediately. If the context contains any commands that refer to (not yet configured) interfaces, those commands fail.

- The filename does not require a file extension, although we recommend using ".cfg". The server must be accessible from the admin context. If the configuration file is not available, you see the following warning message:

  WARNING: Could not fetch the URL url
  INFO: Creating context with default config

- For non-HTTP(S) URL locations, after you specify the URL, you can then change to the context, configure it at the CLI, and enter the `write memory` command to write the file to the URL location. (HTTP(S) is read only).

- The admin context file must be stored on the internal flash memory.

- Available URL types include: `disknumber` (for flash memory), `ftp`, `http`, `https`, or `tftp`.

- To change the URL, reenter the `config-url` command with a new URL. See Change the Security Context URL, page 6-25 for more information about changing the URL.

**Step 7**

(Optional) Assign a context to a failover group in Active/Active failover:

```
join-failover-group { 1 | 2 }
```
Example:

ciscoasa(config-ctx)# join-failover-group 2

By default, contexts are in group 1. The admin context must always be in group 1.

See Configure Optional Failover Parameters, page 7-34 for detailed information about failover groups.

Step 8
(Optional) Enable Cloud Web Security for this context:

```plaintext
scansafe [license key]
```

Example:

ciscoasa(config-ctx)# scansafe

If you do not specify a `license`, the context uses the license configured in the system configuration. The ASA sends the authentication key to the Cloud Web Security proxy servers to indicate from which organization the request comes. The authentication key is a 16-byte hexadecimal number.

See the firewall configuration guide for detailed information about ScanSafe.

Examples

The following example sets the admin context to be “administrator,” creates a context called “administrator” on the internal flash memory, and then adds two contexts from an FTP server:

```plaintext
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115 int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235 int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```
Assign MAC Addresses to Context Interfaces Automatically

This section describes how to configure auto-generation of MAC addresses. The MAC address is used to classify packets within a context. See About MAC Addresses, page 6-11 for more information, especially if you are upgrading from an earlier ASA version. See also View Assigned MAC Addresses, page 6-36.

Guidelines

- When you configure a `nameif` command for the interface in a context, the new MAC address is generated immediately. If you enable this feature after you configure context interfaces, then MAC addresses are generated for all interfaces immediately after you enable it. If you disable this feature, the MAC address for each interface reverts to the default MAC address. For example, subinterfaces of GigabitEthernet 0/1 revert to using the MAC address of GigabitEthernet 0/1.

- In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See Configuring the MAC Address, MTU, and TCP MSS, page 11-9 to manually set the MAC address.

Procedure

Step 1  Automatically assign private MAC addresses to each context interface:

```
mac-address auto [prefix prefix]
```

Example:

```
ciscoasa(config)# mac-address auto prefix 19
```

If you do not enter a prefix, then the ASA autogenerates the prefix based on the last two bytes of the interface (ASA 5500-X) or backplane (ASASM) MAC address.

If you manually enter a prefix, then the `prefix` is a decimal value between 0 and 65535. This prefix is converted to a four-digit hexadecimal number, and used as part of the MAC address. See MAC Address Format, page 6-12 section for more information about how the prefix is used.

Change Between Contexts and the System Execution Space

If you log in to the system execution space (or the admin context), you can change between contexts and perform configuration and monitoring tasks within each context. The running configuration that you edit in a configuration mode, or that is used in the `copy` or `write` commands, depends on your location. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) by entering the `show running-config` command. Only the current configuration displays.

Procedure
Step 1  Change to a context:
\texttt{changeto context \textit{name}}

The prompt changes to the \texttt{ciscoasa/name#}

Step 2  Change to the system execution space:
\texttt{changeto system}

The prompt changes to \texttt{ciscoasa#}

Manage Security Contexts

This section describes how to manage security contexts.

- Remove a Security Context, page 6-24
- Change the Admin Context, page 6-25
- Change the Security Context URL, page 6-25
- Reload a Security Context, page 6-26

Remove a Security Context

You cannot remove the current admin context, unless you remove all contexts using the \texttt{clear context} command.

\textbf{Note}
If you use failover, there is a delay between when you remove the context on the active unit and when the context is removed on the standby unit. You might see an error message indicating that the number of interfaces on the active and standby units are not consistent; this error is temporary and can be ignored.

\textbf{Before You Begin}
Perform this procedure in the system execution space.

\textbf{Procedure}

\textbf{Step 1}  Remove a single context:
\texttt{no context \textit{name}}

All context commands are also removed. The context configuration file is not removed from the config URL location.

\textbf{Step 2}  Remove all contexts (including the admin context):
\texttt{clear context}
The context configuration files are not removed from the config URL locations.

## Change the Admin Context

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 in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users.

### Guidelines

You can set any context to be the admin context, as long as the configuration file is stored in the internal flash memory.

### Before You Begin

Perform this procedure in the system execution space.

### Procedure

**Step 1**  
Set the admin context:

```
admin-context context_name
```

Example:

```
ciscoasa(config)# admin-context administrator
```

Any remote management sessions, such as Telnet, SSH, or HTTPS, that are connected to the admin context are terminated. You must reconnect to the new admin context.

A few system configuration commands, including `ntp server`, identify an interface name that belongs to the admin context. If you change the admin context, and that interface name does not exist in the new admin context, be sure to update any system commands that refer to the interface.

## Change the Security Context URL

This section describes how to change the context URL.

### Guidelines

- You cannot change the security context URL without reloading the configuration from the new URL. The ASA merges the new configuration with the current running configuration.
- Reentering the same URL also merges the saved configuration with the running configuration.
- A merge adds any new commands from the new configuration to the running configuration.
Manage Security Contexts

If the configurations are the same, no changes occur.

If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used.

- If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

**Before You Begin**
Perform this procedure in the system execution space.

**Procedure**

**Step 1** (Optional, if you do not want to perform a merge) Change to the context and clears configuration:

```bash
  changeto context name
  clear configure all
```

Example:

```
ciscoasa(config)# changeto context ctx1
ctxt1(config)# clear configure all
```

If you want to perform a merge, skip to Step 2.

**Step 2** Change to the system execution space:

```bash
  changeto system
```

Example:

```
ciscoasa/ctx1(config)# changeto system
ctxt1(config)#
```

**Step 3** Enters the context configuration mode for the context you want to change.

```bash
  context name
```

Example:

```
ciscoasa(config)# context ctx1
```

**Step 4** Enters the new URL. The system immediately loads the context so that it is running.

```bash
  config-url new_url
```

Example:

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

**Reload a Security Context**

You can reload the context in two ways:

- Clear the running configuration and then import the startup configuration.
This action clears most attributes associated with the context, such as connections and NAT tables.

- Remove the context from the system configuration.

This action clears additional attributes, such as memory allocation, which might be useful for troubleshooting. However, to add the context back to the system requires you to respecify the URL and interfaces.

- **Reload by Clearing the Configuration, page 6-27**
- **Reload by Removing and Re-adding the Context, page 6-27**

**Reload by Clearing the Configuration**

To reload the context by clearing the context configuration and reloading the configuration from the URL, perform the following steps.

**Procedure**

**Step 1**  
Change to the context that you want to reload:

```
changeto context name
```

Example:

```
ciscoasa(config)# changeto context ctx1
```

**Step 2**  
Clear the running configuration:

```
clear configure all
```

This command clears all connections.

**Step 3**  
Reload the configuration:

```
copy startup-config running-config
```

Example:

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

The ASA copies the configuration from the URL specified in the system configuration. You cannot change the URL from within a context.

**Reload by Removing and Re-adding the Context**

To reload the context by removing the context and then re-adding it, perform the steps in the following sections:

1. **Remove a Security Context, page 6-24.**
2. **Configure a Security Context, page 6-19**
Monitoring Security Contexts

This section describes how to view and monitor context information.

- **View Context Information**, page 6-28
- **View Resource Allocation**, page 6-29
- **View Resource Usage**, page 6-32
- **Monitor SYN Attacks in Contexts**, page 6-34
- **View Assigned MAC Addresses**, page 6-36

View Context Information

From the system execution space, you can view a list of contexts including the name, allocated interfaces, and configuration file URL.

From the system execution space, view all contexts by entering the following command:

**Procedure**

**Step 1**

Shows all contexts:

```
show context [name | detail | count]
```

If you want to show information for a particular context, specify the **name**.

The **detail** option shows additional information. See the following sample outputs below for more information.

The **count** option shows the total number of contexts.

The following is sample output from the **show context** command. The following sample output shows three contexts:

```
ciscoasa# show context
Context Name   Interfaces          URL
  *admin       GigabitEthernet0/1.100 disk0:/admin.cfg
               GigabitEthernet0/1.101
  contexta     GigabitEthernet0/1.200 disk0:/contexta.cfg
               GigabitEthernet0/1.201
  contextb     GigabitEthernet0/1.300 disk0:/contextb.cfg
               GigabitEthernet0/1.301
Total active Security Contexts: 3
```

**Table 6-2** shows each field description.
The following is sample output from the `show context detail` command:

ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
Config URL: disk0:/admin.cfg
Real Interfaces: Management0/0
Mapped Interfaces: Management0/0
Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
Config URL: ctx.cfg
Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
GigabitEthernet0/2.30
Mapped Interfaces: int1, int2, int3
Flags: 0x00000011, ID: 2

Context "system", is a system resource
Config URL: startup-config
Real Interfaces:
Mapped Interfaces: Control0/0, GigabitEthernet0/0,
GigabitEthernet0/0.10, GigabitEthernet0/1.10,
GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
GigabitEthernet0/3, Management0/0, Management0/0.1
Flags: 0x00000019, ID: 257

Context "null", is a system resource
Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Flags: 0x00000009, ID: 258

See the command reference for more information about the `detail` output.

The following is sample output from the `show context count` command:

ciscoasa# show context count
Total active contexts: 2

### View Resource Allocation

From the system execution space, you can view the allocation for each resource across all classes and class members.

To view the resource allocation, enter the following command:

**Procedure**

**Step 1** Show the resource allocation:
show resource allocation [detail]

This command shows the resource allocation, but does not show the actual resources being used. See View Resource Usage, page 6-32 for more information about actual resource usage.

The detail argument shows additional information. See the following sample outputs for more information.

The following sample output shows the total allocation of each resource as an absolute value and as a percentage of the available system resources:

ciscoasa# show resource allocation
<table>
<thead>
<tr>
<th>Resource</th>
<th>Total</th>
<th>% of Avail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conns [rate]</td>
<td>35000</td>
<td>N/A</td>
</tr>
<tr>
<td>Inspects [rate]</td>
<td>35000</td>
<td>N/A</td>
</tr>
<tr>
<td>Syslogs [rate]</td>
<td>10500</td>
<td>N/A</td>
</tr>
<tr>
<td>Conns</td>
<td>305000</td>
<td>30.50%</td>
</tr>
<tr>
<td>Hosts</td>
<td>78842</td>
<td>N/A</td>
</tr>
<tr>
<td>SSH</td>
<td>35</td>
<td>35.00%</td>
</tr>
<tr>
<td>Routes</td>
<td>5000</td>
<td>N/A</td>
</tr>
<tr>
<td>Telnet</td>
<td>35</td>
<td>35.00%</td>
</tr>
<tr>
<td>Xlates</td>
<td>91749</td>
<td>N/A</td>
</tr>
<tr>
<td>Other VPN Sessions</td>
<td>20</td>
<td>2.66%</td>
</tr>
<tr>
<td>Other VPN Burst</td>
<td>20</td>
<td>2.66%</td>
</tr>
<tr>
<td>All</td>
<td>unlimited</td>
<td></td>
</tr>
</tbody>
</table>

Table 6-3 shows each field description.

Table 6-3 show resource allocation Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>The name of the resource that you can limit.</td>
</tr>
<tr>
<td>Total</td>
<td>The total amount of the resource that is allocated across all contexts. The amount is an absolute number of concurrent instances or instances per second. If you specified a percentage in the class definition, the ASA converts the percentage to an absolute number for this display.</td>
</tr>
<tr>
<td>% of Avail</td>
<td>The percentage of the total system resources that is allocated across all contexts, if the resource has a hard system limit. If a resource does not have a system limit, this column shows N/A.</td>
</tr>
</tbody>
</table>

The following is sample output from the show resource allocation detail command:

ciscoasa# show resource allocation detail
Resource Origin:
- A Value was derived from the resource 'all'
- C Value set in the definition of this class
- D Value set in default class

<table>
<thead>
<tr>
<th>Resource</th>
<th>Class</th>
<th>Members</th>
<th>Origin</th>
<th>Limit</th>
<th>Total</th>
<th>Total %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conns [rate]</td>
<td></td>
<td>all</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gold</td>
<td>default</td>
<td>1</td>
<td>C</td>
<td>34000</td>
<td>34000</td>
<td>N/A</td>
</tr>
<tr>
<td>silver</td>
<td>gold</td>
<td>1</td>
<td>CA</td>
<td>17000</td>
<td>17000</td>
<td>N/A</td>
</tr>
<tr>
<td>bronze</td>
<td>silver</td>
<td>0</td>
<td>CA</td>
<td>8500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Contexts</td>
<td>bronze</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inspects [rate]</td>
<td></td>
<td>all</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gold</td>
<td>default</td>
<td>1</td>
<td>DA</td>
<td>unlimited</td>
<td>51000</td>
<td>N/A</td>
</tr>
<tr>
<td>silver</td>
<td>gold</td>
<td>1</td>
<td>CA</td>
<td>10000</td>
<td>10000</td>
<td>N/A</td>
</tr>
</tbody>
</table>
bronze             0      CA       5000
All Contexts:      3                          10000     N/A

Syslogs [rate]      default          all      CA  unlimited
gold               1       C     6000       6000     N/A
silver             1      CA     3000       3000     N/A
bronze             0      CA     1500
All Contexts:      3                          9000     N/A

Conns              default          all      CA  unlimited
gold               1       C     200000     200000     20.00%
silver             1      CA     100000     100000     10.00%
bronze             0      CA      50000
All Contexts:      3                        300000     30.00%

Hosts              default          all      CA  unlimited
gold               1       DA  unlimited
silver             1      CA     26214      26214      N/A
bronze             0      CA      13107
All Contexts:      3                         26214      N/A

SSH                default          all       C          5
gold               1       D          5          5      5.00%
silver             1      CA         10         10     10.00%
bronze             0      CA          5
All Contexts:      3                            20     20.00%

Telnet             default          all       C          5
gold               1       D          5          5      5.00%
silver             1      CA         10         10     10.00%
bronze             0      CA          5
All Contexts:      3                            20     20.00%

Routes             default          all       C unlimited N/A
gold               1       D  unlimited 5      N/A
silver             1      CA         10         10     N/A
bronze             0      CA          5
All Contexts:      3                            20     N/A

Xlates             default          all      CA  unlimited
gold               1       DA  unlimited
silver             1      CA     23040      23040     N/A
bronze             0      CA     11520
All Contexts:      3                        23040     N/A

mac-addresses      default          all       C      65535
gold               1       D     65535      65535      100.00%
silver             1      CA     6553      6553      9.99%
bronze             0      CA     3276
All Contexts:      3                        137623    209.99%

Table 6-4 shows each field description.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>The name of the resource that you can limit.</td>
</tr>
<tr>
<td>Class</td>
<td>The name of each class, including the default class.</td>
</tr>
<tr>
<td></td>
<td>The All contexts field shows the total values across all classes.</td>
</tr>
<tr>
<td>Mmbrs</td>
<td>The number of contexts assigned to each class.</td>
</tr>
</tbody>
</table>
Monitoring Security Contexts

View Resource Usage

From the system execution space, you can view the resource usage for each context and display the system resource usage.

Procedure

**Step 1** View resource usage for each context:

```plaintext
show resource usage [context context_name | top n | all | summary | system] [resource (resource_name | all) | detail] [counter counter_name [count_threshold]]
```

- By default, all context usage is displayed; each context is listed separately.
- Enter the `top n` keyword to show the contexts that are the top `n` users of the specified resource. You must specify a single resource type, and not `resource all`, with this option.
- The `summary` option shows all context usage combined.
- The `system` option shows all context usage combined, but shows the system limits for resources instead of the combined context limits.
- For the `resource resource_name`, see Table 6-1 for available resource names. See also the `show resource type` command. Specify `all` (the default) for all types.
- The `detail` option shows the resource usage of all resources, including those you cannot manage. For example, you can view the number of TCP intercepts.
- The `counter counter_name` is one of the following keywords:
  - `current`—Shows the active concurrent instances or the current rate of the resource.

**Table 6-4 show resource allocation detail Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin</td>
<td>The origin of the resource limit, as follows:</td>
</tr>
<tr>
<td></td>
<td>• A—You set this limit with the <code>all</code> option, instead of as an individual resource.</td>
</tr>
<tr>
<td></td>
<td>• C—This limit is derived from the member class.</td>
</tr>
<tr>
<td></td>
<td>• D—This limit was not defined in the member class, but was derived from the default class. For a context assigned to the default class, the value will be “C” instead of “D.”</td>
</tr>
<tr>
<td></td>
<td>The ASA can combine “A” with “C” or “D.”</td>
</tr>
<tr>
<td>Limit</td>
<td>The limit of the resource per context, as an absolute number. If you specified a percentage in the class definition, the ASA converts the percentage to an absolute number for this display.</td>
</tr>
<tr>
<td>Total</td>
<td>The total amount of the resource that is allocated across all contexts in the class. The amount is an absolute number of concurrent instances or instances per second. If the resource is unlimited, this display is blank.</td>
</tr>
<tr>
<td>% of Avail</td>
<td>The percentage of the total system resources that is allocated across all contexts in the class. If the resource is unlimited, this display is blank. If the resource does not have a system limit, then this column shows N/A.</td>
</tr>
</tbody>
</table>
– **denied**—Shows the number of instances that were denied because they exceeded the resource limit shown in the Limit column.

– **peak**—Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the `clear resource usage` command or because the device rebooted.

– **all**—(Default) Shows all statistics.

  - The `count_threshold` sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify `all` for the counter name, then the `count_threshold` applies to the current usage.

  - To show all resources, set the `count_threshold` to 0.

The following is sample output from the `show resource usage context` command, which shows the resource usage for the admin context:

```
ciscoasa# show resource usage context admin
```

<table>
<thead>
<tr>
<th>Resource</th>
<th>Current</th>
<th>Peak</th>
<th>Limit</th>
<th>Denied</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>admin</td>
</tr>
<tr>
<td>Conns</td>
<td>44</td>
<td>55</td>
<td>N/A</td>
<td>0</td>
<td>admin</td>
</tr>
<tr>
<td>Hosts</td>
<td>45</td>
<td>56</td>
<td>N/A</td>
<td>0</td>
<td>admin</td>
</tr>
</tbody>
</table>

The following is sample output from the `show resource usage summary` command, which shows the resource usage for all contexts and all resources. This sample shows the limits for six contexts.

```
ciscoasa# show resource usage summary
```

<table>
<thead>
<tr>
<th>Resource</th>
<th>Current</th>
<th>Peak</th>
<th>Limit</th>
<th>Denied</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslogs [rate]</td>
<td>1743</td>
<td>2132</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>Conns</td>
<td>584</td>
<td>763</td>
<td>280000(S)</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>Xlates</td>
<td>8526</td>
<td>8966</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>Hosts</td>
<td>254</td>
<td>255</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>Conns [rate]</td>
<td>270</td>
<td>535</td>
<td>N/A</td>
<td>1704</td>
<td>Summary</td>
</tr>
<tr>
<td>Inspects [rate]</td>
<td>270</td>
<td>535</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>Other VPN Sessions</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>740</td>
<td>Summary</td>
</tr>
<tr>
<td>Other VPN Burst</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>730</td>
<td>Summary</td>
</tr>
</tbody>
</table>

S = System: Combined context limits exceed the system limit; the system limit is shown.

The following is sample output from the `show resource usage summary` command, which shows the limits for 25 contexts. Because the context limit for Telnet and SSH connections is 5 per context, then the combined limit is 125. The system limit is only 100, so the system limit is shown.

```
ciscoasa# show resource usage summary
```

<table>
<thead>
<tr>
<th>Resource</th>
<th>Current</th>
<th>Peak</th>
<th>Limit</th>
<th>Denied</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>1</td>
<td>1</td>
<td>100(S)</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>SSH</td>
<td>2</td>
<td>2</td>
<td>100(S)</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>Conns</td>
<td>56</td>
<td>90</td>
<td>130000(S)</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>Hosts</td>
<td>89</td>
<td>102</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
</tbody>
</table>

S = System: Combined context limits exceed the system limit; the system limit is shown.

The following is sample output from the `show resource usage system` command, which shows the resource usage for all contexts, but it shows the system limit instead of the combined context limits. The `counter all 0` option is used to show resources that are not currently in use. The Denied statistics indicate how many times the resource was denied due to the system limit, if available.

```
ciscoasa# show resource usage system counter all 0
```

S = System: Combined context limits exceed the system limit; the system limit is shown.
Resource              Current         Peak      Limit        Denied Context
Telnet                      0            0        100             0 System
SSH                         0            0        100             0 System
ASDM                        0            0         32             0 System
Routes                      0            0        N/A             0 System
IPSec                       0 0          5             0 System
Syslogs [rate]              1           18        N/A             0 System
Conns                        0            1     280000             0 System
Xlates                      0            0         N/A             0 System
Hosts                        0            2        N/A             0 System
Conns [rate]                1            1        N/A             0 System
Inspects [rate]             0            0        N/A             0 System
Other VPN Sessions          0           10     750             740 System
Other VPN Burst             0           10     750             730 System

Monitor SYN Attacks in Contexts

The ASA prevents SYN attacks using TCP Intercept. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the ASA acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the ASA receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

Monitor SYN attacks using the following commands:

**Procedure**

**Step 1** Monitor the rate of attacks for individual contexts:

`show perfmon`

**Step 2** Monitor the amount of resources being used by TCP intercept for individual contexts:

`show resource usage detail`

**Step 3** Monitor the resources being used by TCP intercept for the entire system:

`show resource usage summary detail`

The following is sample output from the `show perfmon` command that shows the rate of TCP intercepts for a context called admin.

ciscoasa/admin# show perfmon

```
Context:admin
PERFMON STATS:       Current       Average
Xlates                0/s           0/s
Connections           0/s           0/s
TCP Conns             0/s           0/s
UDP Conns             0/s           0/s
URL Access            0/s           0/s
URL Server Req        0/s           0/s
```
The following is sample output from the `show resource usage detail` command that shows the amount of resources being used by TCP Intercept for individual contexts. (Sample text in **bold** shows the TCP intercept information.)

```
ciscoasa(config)# show resource usage detail
Resource            Current       Peak         Limit       Denied     Context
memory             843732        847288       unlimited     0           admin
chunk:channels       14           15          unlimited     0           admin
chunk:fixup         15           15          unlimited     0           admin
chunk:global         1           1           unlimited     0           admin
chunk:ip-users       10           10          unlimited     0           admin
chunk:list-elem      21           21          unlimited     0           admin
chunk:list-hdr       3            4           unlimited     0           admin
chunk:route          2            2           unlimited     0           admin
 tcp-intercepts   328787        803610       unlimited     0           admin
np-statics          3            3           unlimited     0           admin
stats               1            1           unlimited     0           admin
ace-rules           1            1           unlimited     0           admin
console-access-rul   2            2           unlimited     0           admin
fixup-rules         14           15          unlimited     0           admin
memory             959872        960000       unlimited     0           c1
chunk:channels       15           16          unlimited     0           c1
chunk:dbgtrace       1            1           unlimited     0           c1
chunk:fixup         15           15          unlimited     0           c1
chunk:global         1           1           unlimited     0           c1
chunk:ip-users       2            2           unlimited     0           c1
chunk:list-elem      24           24          unlimited     0           c1
chunk:list-hdr       5            6           unlimited     0           c1
chunk:nat            1            1           unlimited     0           c1
chunk:route          2            2           unlimited     0           c1
 tcp-intercept-rate 16506         16254       unlimited     0           c1
globals              1            1           unlimited     0           c1
np-statics          3            3           unlimited     0           c1
stats               1            1           unlimited     0           c1
nats                1            1           unlimited     0           c1
ace-rules           2            2           unlimited     0           c1
console-access-rul   2            2           unlimited     0           c1
fixup-rules         14           15          unlimited     0           c1
memory             232695716    232020648    unlimited     0           system
chunk:channels       17           20          unlimited     0           system
chunk:dbgtrace       3            3           unlimited     0           system
chunk:fixup         15           15          unlimited     0           system
chunk:ip-users       4            4           unlimited     0           system
chunk:list-elem      1014         1014        unlimited     0           system
chunk:list-hdr       1            1           unlimited     0           system
chunk:route          1            1           unlimited     0           system
 block:16384        510           885         unlimited     0           system
 block:2048          32           34           unlimited     0           system
```
The following sample output shows the resources being used by TCP intercept for the entire system. (Sample text in bold shows the TCP intercept information.)

ciscoasa(config)# show resource usage summary detail

<table>
<thead>
<tr>
<th>Resource</th>
<th>Current</th>
<th>Peak</th>
<th>Limit</th>
<th>Denied</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>238421312</td>
<td>238434336</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:channels</td>
<td>46</td>
<td>48</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:dbgtrace</td>
<td>4</td>
<td>4</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:fixup</td>
<td>45</td>
<td>45</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:global</td>
<td>1</td>
<td>1</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:hole</td>
<td>3</td>
<td>3</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:ip-users</td>
<td>24</td>
<td>24</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:udp-ctrl-blk</td>
<td>1</td>
<td>1</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:list-elem</td>
<td>1059</td>
<td>1059</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:list-hdr</td>
<td>10</td>
<td>11</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:nat</td>
<td>1</td>
<td>1</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:route</td>
<td>5</td>
<td>5</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>chunk:static</td>
<td>2</td>
<td>2</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>block:16384</td>
<td>510</td>
<td>885</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>block:2048</td>
<td>32</td>
<td>35</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>tcp-intercept-rate</td>
<td>341306</td>
<td>811579</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>globals</td>
<td>1</td>
<td>1</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>np-statics</td>
<td>6</td>
<td>6</td>
<td>unlimited</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>statics</td>
<td>2</td>
<td>2</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>nats</td>
<td>1</td>
<td>1</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>ace-rules</td>
<td>3</td>
<td>3</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>console-access-rul</td>
<td>4</td>
<td>4</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
<tr>
<td>fixup-rules</td>
<td>43</td>
<td>44</td>
<td>N/A</td>
<td>0</td>
<td>Summary</td>
</tr>
</tbody>
</table>

View Assigned MAC Addresses

You can view auto-generated MAC addresses within the system configuration or within the context.

- View MAC Addresses in the System Configuration, page 6-36
- View MAC Addresses Within a Context, page 6-38

View MAC Addresses in the System Configuration

This section describes how to view MAC addresses in the system configuration.

Guidelines

If you manually assign a MAC address to an interface, but also have auto-generation enabled, the auto-generated address continues to show in the configuration even though the manual MAC address is the one that is in use. If you later remove the manual MAC address, the auto-generated one shown will be used.

Procedure

Step 1 Show the assigned MAC addresses from the system execution space:

show running-config all context [name]
The **all** option is required to view the assigned MAC addresses. Although the **mac-address auto** command is user-configurable in global configuration mode only, the command appears as a read-only entry in context configuration mode along with the assigned MAC address. Only allocated interfaces that are configured with a **nameif** command within the context have a MAC address assigned.

### Examples

The following output from the `show running-config all context admin` command shows the primary and standby MAC address assigned to the Management0/0 interface:

```
ciscoasa# show running-config all context admin

context admin
 allocates interface Management0/0
 mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
 config-url disk0:/admin.cfg
```

The following output from the `show running-config all context` command shows all the MAC addresses (primary and standby) for all context interfaces. Note that because the GigabitEthernet0/0 and GigabitEthernet0/1 main interfaces are not configured with a **nameif** command inside the contexts, no MAC addresses have been generated for them.

```
ciscoasa# show running-config all context

admin-context admin
 allocates interface Management0/0
 mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
 config-url disk0:/admin.cfg

context CTX1
 allocates interface GigabitEthernet0/0
 allocates interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
 mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
 mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
 mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
 mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
 mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
 allocates interface GigabitEthernet0/1
 allocates interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
 mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
 mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
 mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
 config-url disk0:/CTX1.cfg

context CTX2
 allocates interface GigabitEthernet0/0
 allocates interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
 mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
 mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
 mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
 mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
 mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
 allocates interface GigabitEthernet0/1
 allocates interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
 mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
 mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
```
mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
config-url disk0:/CTX2.cfg
!

View MAC Addresses Within a Context

This section describes how to view MAC addresses within a context.

Procedure

Step 1
Show the MAC address in use by each interface within the context:

```
show interface | include (Interface)| (MAC)
```

Examples

For example:

```
ciscoasa/context# show interface | include (Interface)| (MAC)
```

```
Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
  MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
  MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
  MAC address a201.0103.0600, MTU 1500
...
```

Note

The `show interface` command shows the MAC address in use; if you manually assign a MAC address and also have auto-generation enabled, then you can only view the unused auto-generated address from within the system configuration.

Examples for Multiple Context Mode

The following example:

- Automatically sets the MAC addresses in contexts with a custom prefix.
- Sets the default class limit for conns to 10 percent instead of unlimited, and sets the VPN other sessions to 10, with a burst of 5.
- Creates a gold resource class.
- Sets the admin context to be “administrator.”
- Creates a context called “administrator” on the internal flash memory to be part of the default resource class.
- Adds two contexts from an FTP server as part of the gold resource class.

```
ciscoasa(config)# mac-address auto prefix 19
```

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```
History for Multiple Context Mode

Table 6-5 Feature History for Multiple Context Mode

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple security contexts</td>
<td>7.0(1)</td>
<td>Multiple context mode was introduced. We introduced the following commands: context, mode, and class.</td>
</tr>
<tr>
<td>Automatic MAC address assignment</td>
<td>7.2(1)</td>
<td>Automatic assignment of MAC address to context interfaces was introduced. We introduced the following command: mac-address auto.</td>
</tr>
</tbody>
</table>
### Table 6-5  Feature History for Multiple Context Mode (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource management</td>
<td>7.2(1)</td>
<td>Resource management was introduced. We introduced the following commands: class, limit-resource, and member.</td>
</tr>
<tr>
<td>Virtual sensors for IPS</td>
<td>8.0(2)</td>
<td>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 ASA to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. We introduced the following command: allocate-ips.</td>
</tr>
<tr>
<td>Automatic MAC address assignment</td>
<td>8.0(5)/8.2(2)</td>
<td>The MAC address format was changed to use a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresses are also now persistent across reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2. We modified the following command: mac-address auto prefix.</td>
</tr>
<tr>
<td>Maximum contexts increased for the ASA 5550 and 5580</td>
<td>8.4(1)</td>
<td>The maximum security contexts for the ASA 5550 was increased from 50 to 100. The maximum for the ASA 5580 was increased from 50 to 250.</td>
</tr>
<tr>
<td>Automatic MAC address assignment enabled by default</td>
<td>8.5(1)</td>
<td>Automatic MAC address assignment is now enabled by default. We modified the following command: mac-address auto.</td>
</tr>
</tbody>
</table>
Chapter 6      Multiple Context Mode

History for Multiple Context Mode

Automatic generation of a MAC address prefix 8.6(1) 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 (ASA 5500-X) or backplane (ASASM) MAC address. This conversion happens automatically when you reload, or if you reenable 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 `show running-config mac-address` 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.

Note  To maintain hitless upgrade for failover pairs, the ASA does not 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, especially for the ASASM. 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, reenable MAC address generation to use the default prefix.

We modified the following command: `mac-address auto`.

Dynamic routing in Security Contexts 9.0(1) 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 9.0(1) A new resource type, routes, was created to set the maximum number of routing table entries in each context. We modified the following commands: `limit-resource`, `show resource types`, `show resource usage`, `show resource allocation`.

Table 6-5  Feature History for Multiple Context Mode (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic generation of a MAC address prefix</td>
<td>8.6(1)</td>
<td>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 (ASA 5500-X) or backplane (ASASM) MAC address. This conversion happens automatically when you reload, or if you reenable 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 <code>show running-config mac-address</code> 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. Note To maintain hitless upgrade for failover pairs, the ASA does not 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, especially for the ASASM. 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, reenable MAC address generation to use the default prefix. We modified the following command: <code>mac-address auto</code>.</td>
</tr>
<tr>
<td>Dynamic routing in Security Contexts</td>
<td>9.0(1)</td>
<td>EIGRP and OSPFv2 dynamic routing protocols are now supported in multiple context mode. OSPFv3, RIP, and multicast routing are not supported.</td>
</tr>
<tr>
<td>New resource type for routing table entries</td>
<td>9.0(1)</td>
<td>A new resource type, routes, was created to set the maximum number of routing table entries in each context. We modified the following commands: <code>limit-resource</code>, <code>show resource types</code>, <code>show resource usage</code>, <code>show resource allocation</code>.</td>
</tr>
</tbody>
</table>
### Table 6-5  Feature History for Multiple Context Mode (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-to-Site VPN in multiple context mode</td>
<td>9.0(1)</td>
<td>Site-to-site VPN tunnels are now supported in multiple context mode.</td>
</tr>
</tbody>
</table>
| New resource type for site-to-site VPN tunnels    | 9.0(1)            | 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 commands: `limit-resource`, `show resource types`, `show resource usage`, `show resource allocation`. |
CHAPTER 7

Failover for High Availability

This chapter describes how to configure Active/Standby or Active/Active failover to accomplish high availability of the Cisco ASA.

- **About Failover**, page 7-1
- **Licensing for Failover**, page 7-24
- **Prerequisites for Failover**, page 7-24
- **Guidelines for Failover**, page 7-24
- **Defaults for Failover**, page 7-25
- **Configure Active/Standby Failover**, page 7-25
- **Configure Active/Active Failover**, page 7-29
- **Configure Optional Failover Parameters**, page 7-34
- **Manage Failover**, page 7-41
- **Monitoring Failover**, page 7-47
- **History for Failover**, page 7-48

**About Failover**

- **Failover Overview**, page 7-2
- **Failover System Requirements**, page 7-2
- **Failover and Stateful Failover Links**, page 7-3
- **MAC Addresses and IP Addresses**, page 7-8
- **Intra- and Inter-Chassis Module Placement for the ASA Services Module**, page 7-9
- **Stateless and Stateful Failover**, page 7-12
- **Transparent Firewall Mode Requirements**, page 7-14
- **Failover Health Monitoring**, page 7-16
- **Failover Times**, page 7-18
- **Configuration Synchronization**, page 7-18
- **About Active/Standby Failover**, page 7-20
- **About Active/Active Failover**, page 7-21
Failover Overview

Configuring failover requires two identical ASAs connected to each other through a dedicated failover link and, optionally, a state link. The health of the active units and interfaces is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

The ASA supports two failover modes, Active/Active failover and Active/Standby failover. Each failover mode has its own method for determining and performing failover.

- In Active/Standby failover, one unit is the active unit. It passes traffic. The standby unit does not actively pass traffic. When a failover occurs, the active unit fails over to the standby unit, which then becomes active. You can use Active/Standby failover for ASAs in single or multiple context mode.

- In an Active/Active failover configuration, both ASAs can pass network traffic. Active/Active failover is only available to ASAs in multiple context mode. In Active/Active failover, you divide the security contexts on the ASA into 2 failover groups. A failover group is simply a logical group of one or more security contexts. One group is assigned to be active on the primary ASA, and the other group is assigned to be active on the secondary ASA. When a failover occurs, it occurs at the failover group level.

Both failover modes support stateful or stateless failover.

Failover System Requirements

This section describes the hardware, software, and license requirements for ASAs in a failover configuration.

- Hardware Requirements, page 7-2
- Software Requirements, page 7-2
- License Requirements, page 7-3

Hardware Requirements

The two units in a failover configuration must:

- Be the same model.
- Have the same number and types of interfaces.
- Have the same modules installed (if any)
- Have the same RAM installed.

If you are using units with different flash memory sizes in your failover configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail.

Software Requirements

The two units in a failover configuration must:

- Be in the same firewall mode (routed or transparent).
- Be in the same context mode (single or multiple).
About Failover

- Have the same major (first number) and minor (second number) software version. However, you can temporarily use different versions of the software during an upgrade process; for example, you can upgrade one unit from Version 8.3(1) to Version 8.3(2) and have failover remain active. We recommend upgrading both units to the same version to ensure long-term compatibility.

  See Upgrade a Failover Pair or ASA Cluster, page 36-5 for more information about upgrading the software on a failover pair.

- Have the same AnyConnect images. If the failover pair has mismatched images when a hitless upgrade is performed, then the clientless SSL VPN connection terminates in the final reboot step of the upgrade process, the database shows an orphaned session, and the IP pool shows that the IP address assigned to the client is “in use.”

License Requirements

The two units in a failover configuration do not need to have identical licenses; the licenses combine to make a failover cluster license. See Failover or ASA Cluster Licenses, page 3-23 for more information.

Failover and Stateful Failover Links

The failover link and the optional Stateful Failover link are dedicated connections between the two units.

- Failover Link, page 7-3
- Stateful Failover Link, page 7-4
- Avoiding Interrupted Failover and Data Links, page 7-5

Caution

All information sent over the failover and state links is sent in clear text unless you secure the communication with an IPsec tunnel or a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with an IPsec tunnel or a failover key if you are using the ASA to terminate VPN tunnels.

Failover Link

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit.

- Failover Link Data, page 7-3
- Interface for the Failover Link, page 7-4
- Connecting the Failover Link, page 7-4

Failover Link Data

The following information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization

**Interface for the Failover Link**

You can use any unused interface (physical, redundant, or EtherChannel) as the failover link; however, you cannot specify an interface that is currently configured with a name. The failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface can only be used for the failover link (and optionally also for the state link). The ASA does not support sharing interfaces between user data and the failover link even if different subinterfaces are configured for user data and failover. A separate physical, EtherChannel, or redundant interface must be used for the failover link.

For a redundant interface used as the failover link, see the following benefits for added redundancy:
- When a failover unit boots up, it alternates between the member interfaces to detect an active unit.
- If a failover unit stops receiving keepalive messages from its peer on one of the member interfaces, it switches to the other member interface.

For an EtherChannel used as the failover link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a failover link.

**Connecting the Failover Link**

Connect the failover link in one of the following two ways:
- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the failover interfaces of the ASA.
- Using an Ethernet cable to connect the units directly, without the need for an external switch.

If you do not use a switch between the units, if the interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which unit has the failed interface and caused the link to come down.

The ASA supports Auto-MDI/MDIX on its copper Ethernet ports, so you can either use a crossover cable or a straight-through cable. If you use a straight-through cable, the interface automatically detects the cable and swaps one of the transmit/receive pairs to MDIX.

**Stateful Failover Link**

To use Stateful Failover, you must configure a Stateful Failover link (also known as the state link) to pass connection state information.

You have three interface options for the state link:
- Dedicated Interface (Recommended), page 7-5
- Shared with the Failover Link, page 7-5
- Shared with a Regular Data Interface (Not Recommended), page 7-5

**Note**

Do not use a management interface for the state link.
Dedicated Interface (Recommended)

You can use a dedicated interface (physical, redundant, or EtherChannel) for the state link. For an EtherChannel used as the state link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used.

Connect a dedicated state link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the failover interfaces of the ASA.
- Using an Ethernet cable to connect the appliances directly, without the need for an external switch.

If you do not use a switch between the units, if the interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which unit has the failed interface and caused the link to come down.

The ASA supports Auto-MDI/MDIX on its copper Ethernet ports, so you can either use a crossover cable or a straight-through cable. If you use a straight-through cable, the interface automatically detects the cable and swaps one of the transmit/receive pairs to MDIX.

For optimum performance when using long distance failover, the latency for the failover link should be less than 10 milliseconds and no more than 250 milliseconds. If latency is more than 10 milliseconds, some performance degradation occurs due to retransmission of failover messages.

Shared with the Failover Link

Sharing a failover link might be necessary if you do not have enough interfaces. If you use the failover link as the state link, you should use the fastest Ethernet interface available. If you experience performance problems on that interface, consider dedicating a separate interface for the state link.

Shared with a Regular Data Interface (Not Recommended)

Sharing a data interface with the state link can leave you vulnerable to replay attacks. Additionally, large amounts of Stateful Failover traffic may be sent on the interface, causing performance problems on that network segment.

Using a data interface as the state link is supported in single context, routed mode only.

Avoiding Interrupted Failover and Data Links

We recommend that failover links and data interfaces travel through different paths to decrease the chance that all interfaces fail at the same time. If the failover link is down, the ASA can use the data interfaces to determine if a failover is required. Subsequently, the failover operation is suspended until the health of the failover link is restored.

See the following connection scenarios to design a resilient failover network.

Scenario 1—Not Recommended

If a single switch or a set of switches are used to connect both failover and data interfaces between two ASAs, then when a switch or inter-switch-link is down, both ASAs become active. Therefore, the following two connection methods shown in Figure 7-1 and Figure 7-2 are NOT recommended.
About Failover

Figure 7-1  Connecting with a Single Switch—Not Recommended

Figure 7-2  Connecting with a Double Switch—Not Recommended

Scenario 2—Recommended
We recommend that failover links NOT use the same switch as the data interfaces. Instead, use a different switch or use a direct cable to connect the failover link, as shown in Figure 7-3 and Figure 7-4.

Figure 7-3  Connecting with a Different Switch

Figure 7-4  Connecting with a Cable

Scenario 3—Recommended
If the ASA data interfaces are connected to more than one set of switches, then a failover link can be connected to one of the switches, preferably the switch on the secure (inside) side of network, as shown in Figure 7-5.
Scenario 4—Recommended

The most reliable failover configurations use a redundant interface on the failover link, as shown in Figure 7-6 and Figure 7-7.
MAC Addresses and IP Addresses

When you configure your interfaces, you must specify an active IP address and a standby IP address on the same network.

1. When the primary unit or failover group fails over, the secondary unit assumes the IP addresses and MAC addresses of the primary unit and begins passing traffic.

2. The unit that is now in standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

**Note**

If the secondary unit boots without detecting the primary unit, the secondary unit becomes the active unit and uses its own MAC addresses, because it does not know the primary unit MAC addresses. However, when the primary unit becomes available, the secondary (active) unit changes the MAC addresses to those of the primary unit, which can cause an interruption in your network traffic. Similarly, if you swap out the primary unit with new hardware, a new MAC address is used.

Virtual MAC addresses guard against this disruption because the active MAC addresses are known to the secondary unit at startup, and remain the same in the case of new primary unit hardware. In multiple context mode, the ASA generates virtual active and standby MAC addresses by default. See About MAC Addresses, page 6-11 for more information. In single context mode, you can manually configure virtual MAC addresses; see Configure Active/Active Failover, page 7-29 for more information.

If you do not configure virtual MAC addresses, you might need to clear the ARP tables on connected routers to restore traffic flow. The ASA does not send gratuitous ARPs for static NAT addresses when the MAC address changes, so connected routers do not learn of the MAC address change for these addresses.
Intra- and Inter-Chassis Module Placement for the ASA Services Module

You can place the primary and secondary ASASMs within the same switch or in two separate switches. The following sections describe each option:

- Intra-Chassis Failover, page 7-9
- Inter-Chassis Failover, page 7-10

Intra-Chassis Failover

If you install the secondary ASASM in the same switch as the primary ASASM, you protect against module-level failure. To protect against switch-level failure, as well as module-level failure, see Inter-Chassis Failover, page 7-10.

Even though both ASASMs are assigned the same VLANs, only the active module takes part in networking. The standby module does not pass any traffic.

Figure 7-8 shows a typical intra-switch configuration.
Inter-Chassis Failover

To protect against switch-level failure, you can install the secondary ASASM in a separate switch. The ASASM does not coordinate failover directly with the switch, but it works harmoniously with the switch failover operation. See the switch documentation to configure failover for the switch.

For the best reliability of failover communications between ASASMs, we recommend that you configure an EtherChannel trunk port between the two switches to carry the failover and state VLANs.

For other VLANs, you must ensure that both switches have access to all firewall VLANs, and that monitored VLANs can successfully pass hello packets between both switches.

Figure 7-9 shows a typical switch and ASASM redundancy configuration. The trunk between the two switches carries the failover ASASM VLANs (VLANs 10 and 11).

Note

ASASM failover is independent of the switch failover operation; however, ASASM works in any switch failover scenario.

Figure 7-9 Normal Operation
If the primary ASASM fails, then the secondary ASASM becomes active and successfully passes the firewall VLANs (Figure 7-10).

Figure 7-10  ASASM Failure
If the entire switch fails, as well as the ASASM (such as in a power failure), then both the switch and the ASASM fail over to their secondary units (Figure 7-11).

**Figure 7-11 Switch Failure**

---

**Stateless and Stateful Failover**

The ASA supports two types of failover, stateless and stateful for both the Active/Standby and Active/Active modes.

- Stateless Failover, page 7-13
- Stateful Failover, page 7-13

**Note**

Some configuration elements for clientless SSL VPN (such as bookmarks and customization) use the VPN failover subsystem, which is part of Stateful Failover. You must use Stateful Failover to synchronize these elements between the members of the failover pair. Stateless failover is not recommended for clientless SSL VPN.
Stateless Failover

When a failover occurs, all active connections are dropped. Clients need to reestablish connections when the new active unit takes over.

Note

Some configuration elements for clientless SSL VPN (such as bookmarks and customization) use the VPN failover subsystem, which is part of Stateful Failover. You must use Stateful Failover to synchronize these elements between the members of the failover pair. Stateless (regular) failover is not recommended for clientless SSL VPN.

Stateful Failover

When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit, or in Active/Active failover, between the active and standby failover groups. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

- Supported Features, page 7-13
- Unsupported Features, page 7-14

Supported Features

The following state information is passed to the standby ASA when Stateful Failover is enabled:

- NAT translation table
- TCP connection states
- UDP connection states
- The ARP table
- The Layer 2 bridge table (when running in transparent firewall mode)
- The HTTP connection states (if HTTP replication is enabled)—By default, the ASA does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss.
- The ISAKMP and IPsec SA table
- GTP PDP connection database
- SIP signalling sessions
- ICMP connection state—ICMP connection replication is enabled only if the respective interface is assigned to an asymmetric routing group.
- Dynamic Routing Protocols—Stateful Failover participates in dynamic routing protocols, like OSPF and EIGRP, so routes that are learned through dynamic routing protocols on the active unit are maintained in a Routing Information Base (RIB) table on the standby unit. Upon a failover event, packets travel normally with minimal disruption to traffic because the active secondary ASA initially has rules that mirror the primary ASA. Immediately after failover, the re-convergence timer starts on the newly Active unit. Then the epoch number for the RIB table increments. During re-convergence, OSPF and EIGRP routes become updated with a new epoch number. Once the timer is expired, stale route entries (determined by the epoch number) are removed from the table. The RIB then contains the newest routing protocol forwarding information on the newly Active unit.
Note 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.

- Cisco IP SoftPhone sessions—If a failover occurs during an active Cisco IP SoftPhone session, the call remains active because the call session state information is replicated to the standby unit. When the call is terminated, the IP SoftPhone client loses connection with the Cisco Call Manager. This connection loss occurs because there is no session information for the CTIQBE hangup message on the standby unit. When the IP SoftPhone client does not receive a response back from the Call Manager within a certain time period, it considers the Call Manager unreachable and unregisters itself.

- VPN—VPN end-users do not have to reauthenticate or reconnect the VPN session after a failover. However, applications operating over the VPN connection could lose packets during the failover process and not recover from the packet loss.

Unsupported Features

The following state information is not passed to the standby ASA when Stateful Failover is enabled:

- The HTTP connection table (unless HTTP replication is enabled)
- The user authentication (uauth) table
- Application inspections that are subject to advanced TCP-state tracking—The TCP state of these connections is not automatically replicated. While these connections are replicated to the standby unit, there is a best-effort attempt to re-establish a TCP state.
- TCP state bypass connections
- DHCP server address leases
- Multicast routing
- State information for modules, such as the ASA FirePOWER module.
- Phone proxy connections—When the active unit goes down, the call fails, media stops flowing, and the phone should unregister from the failed unit and reregister with the active unit. The call must be re-established.
- Selected clientless SSL VPN features:
  - Smart Tunnels
  - Port Forwarding
  - Plugins
  - Java Applets
  - IPv6 clientless or Anyconnect sessions
  - Citrix authentication (Citrix users must reauthenticate after failover)

Transparent Firewall Mode Requirements

- Transparent Mode Requirements for Appliances, page 7-15
- Transparent Mode Requirements for Modules, page 7-15
Transparent Mode Requirements for Appliances

When the active unit fails over to the standby unit, the connected switch port running Spanning Tree Protocol (STP) can go into a blocking state for 30 to 50 seconds when it senses the topology change. To avoid traffic loss while the port is in a blocking state, you can configure one of the following workarounds depending on the switch port mode:

- **Access mode**—Enable the STP PortFast feature on the switch:

  ```
  interface interface_id
  spanning-tree portfast
  ```

  The PortFast feature immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

- **Trunk mode**—Block BPDUs on the ASA on both the inside and outside interfaces with an EtherType access rule.

  ```
  access-list id ethertype deny bpdu
  access-group id in interface inside_name
  access-group id in interface outside_name
  ```

  Blocking BPDUs disables STP on the switch. Be sure not to have any loops involving the ASA in your network layout.

If neither of the above options are possible, then you can use one of the following less desirable workarounds that impacts failover functionality or STP stability:

- Disable interface monitoring.
- Increase interface holdtime to a high value that will allow STP to converge before the ASAs fail over.
- Decrease STP timers to allow STP to converge faster than the interface holdtime.

Transparent Mode Requirements for Modules

To avoid loops when you use failover in transparent mode, you should allow BPDUs to pass (the default), and you must use switch software that supports BPDU forwarding.

Loops can occur if both modules are active at the same time, such as when both modules are discovering each other’s presence, or due to a bad failover link. Because the ASASMs bridge packets between the same two VLANs, loops can occur when inside packets destined for the outside get endlessly replicated by both ASASMs (see Figure 7-12). The spanning tree protocol can break such loops if there is a timely exchange of BPDUs. To break the loop, BPDUs sent between VLAN 200 and VLAN 201 need to be bridged.
Failover Health Monitoring

The ASA monitors each unit for overall health and for interface health. This section includes information about how the ASA performs tests to determine the state of each unit.

- Unit Health Monitoring, page 7-16
- Interface Monitoring, page 7-17

Unit Health Monitoring

The ASA determines the health of the other unit by monitoring the failover link with hello messages. When a unit does not receive three consecutive hello messages on the failover link, the unit sends LANTEST messages on each data interface, including the failover link, to validate whether or not the peer is responsive. The action that the ASA takes depends on the response from the other unit. See the following possible actions:

- If the ASA receives a response on the failover link, then it does not fail over.
- If the ASA does not receive a response on the failover link, but it does receive a response on a data interface, then the unit does not failover. The failover link is marked as failed. You should restore the failover link as soon as possible because the unit cannot fail over to the standby while the failover link is down.
- If the ASA does not receive a response on any interface, then the standby unit switches to active mode and classifies the other unit as failed.
Interface Monitoring

You can monitor up to 250 interfaces (in multiple mode, divided between all contexts). You should monitor important interfaces. For example in multiple mode, you might configure one context to monitor a shared interface: because the interface is shared, all contexts benefit from the monitoring.

When a unit does not receive hello messages on a monitored interface for 2 polling periods, it runs interface tests. If all interface tests fail for an interface, but this same interface on the other unit continues to successfully pass traffic, then the interface is considered to be failed. If the threshold for failed interfaces is met, then a failover occurs. If the other unit interface also fails all the network tests, then both interfaces go into the “Unknown” state and do not count towards the failover limit.

An interface becomes operational again if it receives any traffic. A failed ASA returns to standby mode if the interface failure threshold is no longer met.

If you have a services module, such as the ASA FirePOWER SSP, then the ASA also monitors the health of the module over the backplane interface. Failure of the module is considered a unit failure and will trigger failover. This setting is configurable.

If an interface has IPv4 and IPv6 addresses configured on it, the ASA uses the IPv4 addresses to perform the health monitoring.

If an interface has only IPv6 addresses configured on it, then the ASA uses IPv6 neighbor discovery instead of ARP to perform the health monitoring tests. For the broadcast ping test, the ASA uses the IPv6 all nodes address (FE02::1).

Note

If a failed unit does not recover and you believe it should not be failed, you can reset the state by entering the `failover reset` command. If the failover condition persists, however, the unit will fail again.

Interface Tests

The ASA uses the following interface tests:

1. Link Up/Down test—A test of the interface status. If the Link Up/Down test indicates that the interface is down, then the ASA considers it failed. If the status is Up, then the ASA performs the Network Activity test.

2. Network Activity test—A received network activity test. The purpose of this test is to generate network traffic using LANTEST messages to determine which (if either) unit has failed. At the start of the test, each unit clears its received packet count for its interfaces. As soon as a unit receives any packets during the test (up to 5 seconds), then the interface is considered operational. If one unit receives traffic and the other unit does not, then the unit that received no traffic is considered failed. If neither unit receives traffic, then the ASA starts the ARP test.

3. ARP test—A reading of the unit ARP cache for the 10 most recently acquired entries. One at a time, the unit sends ARP requests to these machines, attempting to stimulate network traffic. After each request, the unit counts all received traffic for up to 5 seconds. If traffic is received, the interface is considered operational. If no traffic is received, an ARP request is sent to the next machine. If at the end of the list no traffic has been received, the ASA starts the ping test.

4. Broadcast Ping test—A ping test that consists of sending out a broadcast ping request. The unit then counts all received packets for up to 5 seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops. If no traffic is received, the testing starts over again with the ARP test.
Interface Status

Monitored interfaces can have the following status:

- **Unknown**—Initial status. This status can also mean the status cannot be determined.
- **Normal**—The interface is receiving traffic.
- **Testing**—Hello messages are not heard on the interface for five poll times.
- **Link Down**—The interface or VLAN is administratively down.
- **No Link**—The physical link for the interface is down.
- **Failed**—No traffic is received on the interface, yet traffic is heard on the peer interface.

Failover Times

Table 7-1 shows the minimum, default, and maximum failover times.

**Table 7-1 ASA Failover Times**

<table>
<thead>
<tr>
<th>Failover Condition</th>
<th>Minimum</th>
<th>Default</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active unit loses power or stops normal operation.</td>
<td>800 milliseconds</td>
<td>15 seconds</td>
<td>45 seconds</td>
</tr>
<tr>
<td>Active unit main board interface link down.</td>
<td>500 milliseconds</td>
<td>5 seconds</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Active unit 4GE module interface link down.</td>
<td>2 seconds</td>
<td>5 seconds</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Active unit IPS or CSC module fails.</td>
<td>2 seconds</td>
<td>2 seconds</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Active unit interface up, but connection problem causes interface testing.</td>
<td>5 seconds</td>
<td>25 seconds</td>
<td>75 seconds</td>
</tr>
</tbody>
</table>

Configuration Synchronization

Failover includes two types of configuration synchronization:

- **Running Configuration Replication**, page 7-18
- **File Replication**, page 7-19
- **Command Replication**, page 7-19

Running Configuration Replication

Running configuration replication occurs when one or both devices in the failover pair boot. Configurations are always synchronized from the active unit to the standby unit. When the standby unit completes its initial startup, it clears its running configuration (except for the failover commands needed to communicate with the active unit), and the active unit sends its entire configuration to the standby unit.

When the replication starts, the ASA console on the active unit displays the message “Beginning configuration replication: Sending to mate,” and when it is complete, the ASA displays the message “End Configuration Replication to mate.” Depending on the size of the configuration, replication can take from a few seconds to several minutes.

On the standby unit, the configuration exists only in running memory. You should save the configuration to flash memory according to **Save Configuration Changes**, page 2-17.
Note
During replication, commands entered on the active unit may not replicate properly to the standby unit, and commands entered on the standby unit may be overwritten by the configuration being replicated from the active unit. Avoid entering commands on either unit during the configuration replication process.

Note
The `crypto ca server` command and related sub commands are not synchronized to the failover peer.

**File Replication**

Configuration syncing does not replicate the following files and configuration components, so you must copy these files manually so they match:

- AnyConnect images
- CSD images
- AnyConnect profiles

The ASA uses a cached file for the AnyConnect client profile stored in `cache:/stc/profiles`, and not the file stored in the flash file system. To replicate the AnyConnect client profile to the standby unit, perform one of the following:
  - Enter the `write standby` command on the active unit.
  - Reapply the profile on the active unit.
  - Reload the standby unit.

- Local Certificate Authorities (CAs)
- ASA images
- ASDM images

**Command Replication**

After startup, commands that you enter on the active unit are immediately replicated to the standby unit. You do not have to save the active configuration to flash memory to replicate the commands.

In Active/Active failover, commands entered in the system execution space are replicated from the unit on which failover group 1 is in the active state.

Failure to enter the commands on the appropriate unit for command replication to occur causes the configurations to be out of synchronization. Those changes may be lost the next time the initial configuration synchronization occurs.

The following commands are replicated to the standby ASA:

- All configuration commands except for `mode`, `firewall`, and `failover lan unit`
- `copy running-config startup-config`
- `delete`
- `mkdir`
- `rename`
- `rmdir`
About Failover

The following commands are *not* replicated to the standby ASA:

- All forms of the `copy` command except for `copy running-config startup-config`
- All forms of the `write` command except for `write memory`
- `debug`
- `failover lan unit`
- `firewall`
- `show`
- `terminal pager` and `pager`

About Active/Standby Failover

Active/Standby failover lets you use a standby ASA to take over the functionality of a failed unit. When the active unit fails, it changes to the standby state while the standby unit changes to the active state.

**Note**

For multiple context mode, the ASA can fail over the entire unit (including all contexts) but cannot fail over individual contexts separately.

- Primary/Secondary Roles and Active/Standby Status, page 7-20
- Active Unit Determination at Startup, page 7-20
- Failover Events, page 7-21

Primary/Secondary Roles and Active/Standby Status

The main differences between the two units in a failover pair are related to which unit is active and which unit is standby, namely which IP addresses to use and which unit actively passes traffic.

However, a few differences exist between the units based on which unit is primary (as specified in the configuration) and which unit is secondary:

- The primary unit always becomes the active unit if both units start up at the same time (and are of equal operational health).
- The primary unit MAC addresses are always coupled with the active IP addresses. The exception to this rule occurs when the secondary unit is active and cannot obtain the primary unit MAC addresses over the failover link. In this case, the secondary unit MAC addresses are used.

Active Unit Determination at Startup

The active unit is determined by the following:

- If a unit boots and detects a peer already running as active, it becomes the standby unit.
- If a unit boots and does not detect a peer, it becomes the active unit.
- If both units boot simultaneously, then the primary unit becomes the active unit, and the secondary unit becomes the standby unit.
Failover Events

In Active/Standby failover, failover occurs on a unit basis. Even on systems running in multiple context mode, you cannot fail over individual or groups of contexts.

Table 7-2 shows the failover action for each failure event. For each failure event, the table shows the failover policy (failover or no failover), the action taken by the active unit, the action taken by the standby unit, and any special notes about the failover condition and actions.

Table 7-2 Failover Behavior

<table>
<thead>
<tr>
<th>Failure Event</th>
<th>Policy</th>
<th>Active Action</th>
<th>Standby Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active unit failed (power or hardware)</td>
<td>Failover</td>
<td>n/a</td>
<td>Become active</td>
<td>Mark active as failed. No hello messages are received on any monitored interface or the failover link.</td>
</tr>
<tr>
<td>Formerly active unit recovers</td>
<td>No failover</td>
<td>Become standby</td>
<td>No action</td>
<td>None.</td>
</tr>
<tr>
<td>Standby unit failed (power or hardware)</td>
<td>No failover</td>
<td>Mark standby as failed</td>
<td>n/a</td>
<td>When the standby unit is marked as failed, then the active unit does not attempt to fail over, even if the interface failure threshold is surpassed.</td>
</tr>
<tr>
<td>Failover link failed during operation</td>
<td>No failover</td>
<td>Mark failover link as failed</td>
<td>Mark failover link as failed</td>
<td>You should restore the failover link as soon as possible because the unit cannot fail over to the standby unit while the failover link is down.</td>
</tr>
<tr>
<td>Failover link failed at startup</td>
<td>No failover</td>
<td>Mark failover link as failed</td>
<td>Become active</td>
<td>If the failover link is down at startup, both units become active.</td>
</tr>
<tr>
<td>State link failed</td>
<td>No failover</td>
<td>No action</td>
<td>No action</td>
<td>State information becomes out of date, and sessions are terminated if a failover occurs.</td>
</tr>
<tr>
<td>Interface failure on active unit above threshold</td>
<td>Failover</td>
<td>Mark active as failed</td>
<td>Become active</td>
<td>None.</td>
</tr>
<tr>
<td>Interface failure on standby unit above threshold</td>
<td>No failover</td>
<td>No action</td>
<td>Mark standby as failed</td>
<td>When the standby unit is marked as failed, then the active unit does not attempt to fail over even if the interface failure threshold is surpassed.</td>
</tr>
</tbody>
</table>

About Active/Active Failover

This section describes Active/Active failover.

- Active/Active Failover Overview, page 7-22
- Primary/Secondary Roles and Active/Standby Status for a Failover Group, page 7-22
- Failover Events, page 7-23
About Failover

Active/Active Failover Overview

In an Active/Active failover configuration, both ASAs can pass network traffic. Active/Active failover is only available to ASAs in multiple context mode. In Active/Active failover, you divide the security contexts on the ASA into a maximum of 2 failover groups.

A failover group is simply a logical group of one or more security contexts. You can assign failover group to be active on the primary ASA, and failover group 2 to be active on the secondary ASA. When a failover occurs, it occurs at the failover group level. For example, depending on interface failure patterns, it is possible for failover group 1 to fail over to the secondary ASA, and subsequently failover group 2 to fail over to the primary ASA. This event could occur if the interfaces in failover group 1 are down on the primary ASA but up on the secondary ASA, while the interfaces in failover group 2 are down on the secondary ASA but up on the primary ASA.

The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default. If you want Active/Active failover, but are otherwise uninterested in multiple contexts, the simplest configuration would be to add one additional context and assign it to failover group 2.

Note

When configuring Active/Active failover, make sure that the combined traffic for both units is within the capacity of each unit.

Note

You can assign both failover groups to one ASA if desired, but then you are not taking advantage of having two active ASAs.

Primary/Secondary Roles and Active/Standby Status for a Failover Group

As in Active/Standby failover, one unit in an Active/Active failover pair is designated the primary unit, and the other unit the secondary unit. Unlike Active/Standby failover, this designation does not indicate which unit becomes active when both units start simultaneously. Instead, the primary/secondary designation does two things:

- The primary unit provides the running configuration to the pair when they boot simultaneously.
- Each failover group in the configuration is configured with a primary or secondary unit preference.

Active Unit Determination for Failover Groups at Startup

The unit on which a failover group becomes active is determined as follows:

- When a unit boots while the peer unit is not available, both failover groups become active on the unit.
- When a unit boots while the peer unit is active (with both failover groups in the active state), the failover groups remain in the active state on the active unit regardless of the primary or secondary preference of the failover group until one of the following occurs:
  - A failover occurs.
  - You manually force a failover.
  - You configured preemption for the failover group, which causes the failover group to automatically become active on the preferred unit when the unit becomes available.
When both units boot at the same time, each failover group becomes active on its preferred unit after the configurations have been synchronized.

### Failover Events

In an Active/Active failover configuration, failover occurs on a failover group basis, not a system basis. For example, if you designate both failover groups as active on the primary unit, and failover group 1 fails, then failover group 2 remains active on the primary unit while failover group 1 becomes active on the secondary unit.

Because a failover group can contain multiple contexts, and each context can contain multiple interfaces, it is possible for all interfaces in a single context to fail without causing the associated failover group to fail.

Table 7-3 shows the failover action for each failure event. For each failure event, the policy (whether or not failover occurs), actions for the active failover group, and actions for the standby failover group are given.

### Table 7-3 Failover Behavior for Active/Active Failover

<table>
<thead>
<tr>
<th>Failure Event</th>
<th>Policy</th>
<th>Active Group Action</th>
<th>Standby Group Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A unit experiences a power or software failure</td>
<td>Failover</td>
<td>Become standby</td>
<td>Mark as failed</td>
<td>When a unit in a failover pair fails, any active failover groups on that unit are marked as failed and become active on the peer unit.</td>
</tr>
<tr>
<td>Interface failure on active failover group above threshold</td>
<td>Failover</td>
<td>Mark active group as failed</td>
<td>Become active</td>
<td>None.</td>
</tr>
<tr>
<td>Interface failure on standby failover group above threshold</td>
<td>No failover</td>
<td>No action</td>
<td>Mark standby group as failed</td>
<td>When the standby failover group is marked as failed, the active failover group does not attempt to fail over, even if the interface failure threshold is surpassed.</td>
</tr>
<tr>
<td>Formerly active failover group recovers</td>
<td>No failover</td>
<td>No action</td>
<td>No action</td>
<td>Unless failover group preemption is configured, the failover groups remain active on their current unit.</td>
</tr>
<tr>
<td>Failover link failed at startup</td>
<td>No failover</td>
<td>Become active</td>
<td>Become active</td>
<td>If the failover link is down at startup, both failover groups on both units become active.</td>
</tr>
<tr>
<td>State link failed</td>
<td>No failover</td>
<td>No action</td>
<td>No action</td>
<td>State information becomes out of date, and sessions are terminated if a failover occurs.</td>
</tr>
<tr>
<td>Failover link failed during operation</td>
<td>No failover</td>
<td>n/a</td>
<td>n/a</td>
<td>Each unit marks the failover link as failed. You should restore the failover link as soon as possible because the unit cannot fail over to the standby unit while the failover link is down.</td>
</tr>
</tbody>
</table>
Licensing for Failover

Failover units do not require the same license on each unit. If you have licenses on both units, they combine into a single running failover cluster license. There are some exceptions to this rule. See the following table for precise licensing requirements for failover.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>• Active/Standby—Security Plus License.</td>
</tr>
<tr>
<td></td>
<td>• Active/Active—No Support.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>ASA 5512-X through ASA 5555-X</td>
<td>• ASA 5512-X—Security Plus License.</td>
</tr>
<tr>
<td></td>
<td>• Other models—Base License.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Each unit must have the same encryption license; each unit must have the same IPS module license. You also need the IPS signature subscription on the IPS side for both units. See the following guidelines:</td>
</tr>
<tr>
<td></td>
<td>– To buy the IPS signature subscription you need to have the ASA with IPS pre-installed (the part number must include “IPS”, for example ASA5515-IPS-K9); you cannot buy the IPS signature subscription for a non-IPS part number ASA.</td>
</tr>
<tr>
<td></td>
<td>– You need the IPS signature subscription on both units; this subscription is not shared in failover, because it is not an ASA license.</td>
</tr>
<tr>
<td></td>
<td>– The IPS signature subscription requires a unique IPS module license per unit. Like other ASA licenses, the IPS module license is technically shared in the failover cluster license. However, because of the IPS signature subscription requirements, you must buy a separate IPS module license for each unit in.</td>
</tr>
<tr>
<td>ASAv</td>
<td>• Active/Standby—Standard and Premium Licenses.</td>
</tr>
<tr>
<td></td>
<td>• Active/Active—No Support.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The standby unit requires the same model license as the primary unit; Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>All other models</td>
<td>Base License.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Each unit must have the same encryption license.</td>
</tr>
</tbody>
</table>

Prerequisites for Failover

See Failover System Requirements, page 7-2.

Guidelines for Failover

Context Mode Guidelines

• Active/Standby mode is supported in single and multiple context mode.
• Active/Active mode is supported only in multiple context mode.
• For multiple context mode, perform all steps in the system execution space unless otherwise noted.
• ASA failover replication fails if you try to make a configuration change in two or more contexts at the same time. The workaround is to make configuration changes in each context sequentially.

Additional Guidelines and Limitations
• Configuring port security on the switch(es) connected to an ASA failover pair can cause communication problems when a failover event occurs. This problem occurs when a secure MAC address configured or learned on one secure port moves to another secure port, a violation is flagged by the switch port security feature.
• You can monitor up to 250 interfaces on a unit, across all contexts.
• For Active/Active failover, no two interfaces in the same context should be configured in the same ASR group.
• For Active/Active failover, you can define a maximum of two failover groups.
• For Active/Active failover, when removing failover groups, you must remove failover group 1 last. Failover group 1 always contains the admin context. Any context not assigned to a failover group defaults to failover group 1. You cannot remove a failover group that has contexts explicitly assigned to it.

Related Topics
• Auto Update Server Support in Failover Configurations, page 36-42

Defaults for Failover

By default, the failover policy consists of the following:
• No HTTP replication in Stateful Failover.
• A single interface failure causes failover.
• The interface poll time is 5 seconds.
• The interface hold time is 25 seconds.
• The unit poll time is 1 second.
• The unit hold time is 15 seconds.
• Virtual MAC addresses are enabled in multiple context mode; in single context mode, they are disabled.
• Monitoring on all physical interfaces, or for the ASASM, all VLAN interfaces.

Configure Active/Standby Failover

• Configure the Primary Unit for Active/Standby Failover, page 7-25
• Configure the Secondary Unit for Active/Standby Failover, page 7-29

Configure the Primary Unit for Active/Standby Failover

Follow the steps in this section to configure the primary in an Active/Standby failover configuration. These steps provide the minimum configuration needed to enable failover on the primary unit.
Configure Active/Standby Failover

Before You Begin
- Configure standby IP addresses for all interfaces except for the failover and state links.
- Do not configure a nameif for the failover and state links.
- For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the changeto system command.

Procedure

Step 1
Designate this unit as the primary unit:

```plaintext
failover lan unit primary
```

Step 2
Specify the interface to be used as the failover link:

```plaintext
failover lan interface if_name interface_id
```

Example:

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

This interface cannot be used for any other purpose (except, optionally, the state link). The if_name argument assigns a name to the interface.

The interface_id argument can be a physical interface, subinterface, redundant interface, or EtherChannel interface ID. On the ASASM, the interface_id specifies a VLAN ID.

Step 3
Assign the active and standby IP addresses to the failover link:

```plaintext
failover interface ip failover_if_name {ip_address mask | ipv6_address/prefix} standby ip_address
```

Example:

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Or:

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71
```

This address should be on an unused subnet. The standby IP address must be in the same subnet as the active IP address.

Step 4
Enable the failover link:

```plaintext
interface failover_interface_id
    no shutdown
```

Example:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

Step 5
(Optional) Specify the interface you want to use as the state link:

```plaintext
failover link if_name interface_id
```

Example:

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```
We recommend specifying a separate interface from the failover link or data interfaces. The `if_name` argument assigns a name to the interface.

The `interface_id` argument can be a physical interface, subinterface, redundant interface, or EtherChannel interface ID. On the ASASM, the `interface_id` specifies a VLAN ID.

**Step 6**  
If you specified a separate state link, assign the active and standby IP addresses to the state link:

```
failover interface ip state_if_name (ip_address mask | ipv6_address/prefix) standby ip_address
```

Example:

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
```

Or:

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby 2001:a0a:b00:a::a0a:b71
```

This address should be on an unused subnet, different from the failover link. The standby IP address must be in the same subnet as the active IP address. Skip this step if you are sharing the state link.

**Step 7**  
If you specified a separate state link, enables the state link.

```
interface state_interface_id
no shutdown
```

Example:

```
ciscoasa(config)# interface gigabitethernet 0/4
```

```
ciscoasa(config-if)# no shutdown
```

Skip this step if you are sharing the state link.

**Step 8**  
(Optional) Do one of the following to encrypt communications on the failover and state links:

- (Preferred) Establish IPsec LAN-to-LAN tunnels on the failover and state links between the units to encrypt all failover communications:

  ```
  failover ipsec pre-shared-key [0 | 8] key
  ```

  Example:

  ```
ciscoasa(config)# failover ipsec pre-shared-key a3rynrsun
  ```

  The `key` can be up to 128 characters in length. Identify the same key on both units. The key is used by IKEv2 to establish the tunnels.

  If you use a master passphrase (see Configure the Master Passphrase, page 14-10), then the key is encrypted in the configuration. If you are copying from the configuration (for example, from `more system:running-config` output), specify that the key is encrypted by using the `8` keyword. `0` is used by default, specifying an unencrypted password.

  The `failover ipsec pre-shared-key` shows as ***** in `show running-config` output; this obscured key is not copyable.

  If you do not configure failover and state link encryption, failover communication, including any passwords or keys in the configuration that are sent during command replication, will be in clear text.
You cannot use both IPsec encryption and the legacy \texttt{failover key} encryption. If you configure both methods, IPsec is used. However, if you use the master passphrase (see \textit{Configure the Master Passphrase, page 14-10}), you must first remove the failover key using the \texttt{no failover key} command before you configure IPsec encryption.

Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.

- (Optional) Encrypt failover communication on the failover and state links:
  \begin{verbatim}
  failover key [0 | 8] \{ hex key | shared_secret \}
  \end{verbatim}

  Example:
  \texttt{ciscoasa(config)# failover key johnclicht0n}

  Use a \textit{shared_secret} from 1 to 63 characters or a 32-character \textit{hex key}. For the \textit{shared_secret}, you can use any combination of numbers, letters, or punctuation. The shared secret or hex key is used to generate the encryption key. Identify the same key on both units.

  If you use a master passphrase (see \textit{Configure the Master Passphrase, page 14-10}), then the shared secret or hex key is encrypted in the configuration. If you are copying from the configuration (for example, from \texttt{more system:running-config} output), specify that the shared secret or hex key is encrypted by using the \texttt{8} keyword. \texttt{0} is used by default, specifying an unencrypted password.

  The \texttt{failover key} shared secret shows as ***** in \texttt{show running-config} output; this obscured key is not copyable.

  If you do not configure failover and state link encryption, failover communication, including any passwords or keys in the configuration that are sent during command replication, will be in clear text.

\begin{tabular}{ll}
\textbf{Step 9} & Enable failover: \\
 & \texttt{failover} \\
\textbf{Step 10} & Save the system configuration to flash memory: \\
 & \texttt{write memory} \\
\end{tabular}

\textbf{Examples}

The following example configures the failover parameters for the primary unit:

\begin{verbatim}
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover ipsec pre-shared-key a3rynsun
failover
\end{verbatim}

\textbf{Related Topics}

- Chapter 11, “Routed Mode Interfaces,”
- Chapter 12, “Transparent Mode Interfaces.”
Configure the Secondary Unit for Active/Standby Failover

The only configuration required on the secondary unit is for the failover link. The secondary unit requires these commands to communicate initially with the primary unit. After the primary unit sends its configuration to the secondary unit, the only permanent difference between the two configurations is the failover lan unit command, which identifies each unit as primary or secondary.

Before You Begin
- Do not configure a nameif for the failover and state links.
- For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the changeto system command.

Procedure

Step 1 Re-enter the exact same commands as on the primary unit except for the failover lan unit primary command. You can optionally replace it with the failover lan unit secondary command, but it is not necessary because secondary is the default setting. See Configure the Primary Unit for Active/Standby Failover, page 7-25.

For example:

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
```
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
```
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```
ciscoasa(config)# failover
```

Step 2 After the failover configuration syncs, save the configuration to flash memory:
```
ciscoasa(config)# write memory
```

Configure Active/Active Failover

- Configure the Primary Unit for Active/Active Failover, page 7-29
- Configure the Secondary Unit for Active/Active Failover, page 7-33

Configure the Primary Unit for Active/Active Failover

Follow the steps in this section to configure the primary unit in an Active/Active failover configuration. These steps provide the minimum configuration needed to enable failover on the primary unit.
Configure Active/Active Failover

Before You Begin

- Enable multiple context mode according to Enable or Disable Multiple Context Mode, page 6-15.
- Configure standby IP addresses for all interfaces except for the failover and state links according to Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”
- Do not configure a nameif for the failover and state links.
- Complete this procedure in the system execution space. To change from the context to the system execution space, enter the changeto system command.

Procedure

Step 1
Designate this unit as the primary unit:

```
failover lan unit primary
```

Step 2
Specify the interface to be used as the failover link:

```
failover lan interface if_name interface_id
```

Example:

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

This interface cannot be used for any other purpose (except, optionally, the state link).
The `if_name` argument assigns a name to the interface.
The `interface_id` argument can be a physical interface, subinterface, redundant interface, or EtherChannel interface ID. On the ASASM, the `interface_id` specifies a VLAN ID.

Step 3
Assign the active and standby IP addresses to the failover link:

```
failover interface ip if_name (ip_address mask | ipv6_address/prefix) standby ip_address
```

Example:

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Or:

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71
```

This address should be on an unused subnet.
The standby IP address must be in the same subnet as the active IP address.

Step 4
Enable the failover link:

```
interface failover_interface_id
  no shutdown
```

Example:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

Step 5
(Optional) Specify the interface you want to use as the state link:

```
failover link if_name interface_id
```

Example:

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```
We recommend specifying a separate interface from the failover link or data interfaces.

The interface_name argument assigns a name to the interface.

The interface_id argument can be a physical interface, subinterface, redundant interface, or EtherChannel interface ID. On the ASASM, the interface_id specifies a VLAN ID.

**Step 6**

If you specified a separate state link, assign the active and standby IP addresses to the state link:

This address should be on an unused subnet, different from the failover link.

The standby IP address must be in the same subnet as the active IP address.

Skip this step if you are sharing the state link.

```
failover interface ip state_if_name {ip_address mask | ipv6_address/prefix} standby
ip_address
```

Example:

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

Or:

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

**Step 7**

If you specified a separate state link, enable the state link:

```
interface state_interface_id
no shutdown
```

Example:

```
ciscoasa(config)# interface gigabitethernet 0/4

ciscoasa(config-if)# no shutdown
```

Skip this step if you are sharing the state link.

**Step 8**

(Optional) Do one of the following to encrypt communications on the failover and state links:

- (Preferred) Establish IPsec LAN-to-LAN tunnels on the failover and state links between the units to encrypt all failover communications:

```
failover ipsec pre-shared-key [0 | 8] key
```

Example:

```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

The key can be up to 128 characters in length. Identify the same key on both units. The key is used by IKEv2 to establish the tunnels.

If you use a master passphrase (see Configure the Master Passphrase, page 14-10), then the key is encrypted in the configuration. If you are copying from the configuration (for example, from more system:running-config output), specify that the key is encrypted by using the 8 keyword. 0 is used by default, specifying an unencrypted password.

The failover ipsec pre-shared-key shows as ***** in show running-config output; this obscured key is not copyable.

If you do not configure failover and state link encryption, failover communication, including any passwords or keys in the configuration that are sent during command replication, will be in clear text.
You cannot use both IPsec encryption and the legacy failover key encryption. If you configure both methods, IPsec is used. However, if you use the master passphrase (see Configure the Master Passphrase, page 14-10), you must first remove the failover key using the no failover key command before you configure IPsec encryption.

Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.

- (Optional) Encrypt failover communication on the failover and state links:
  
  \[ \text{failover key [0 | 8] (hex key | shared_secret)} \]

  Example:
  
  ciscoasa(config)# failover key johncricht0n

  Use a shared_secret, from 1 to 63 characters, or a 32-character hex key.

  For the shared_secret, you can use any combination of numbers, letters, or punctuation. The shared secret or hex key is used to generate the encryption key. Identify the same key on both units.

  If you use a master passphrase (see Configure the Master Passphrase, page 14-10), then the shared secret or hex key is encrypted in the configuration. If you are copying from the configuration (for example, from more system:running-config output), specify that the shared secret or hex key is encrypted by using the 8 keyword. 0 is used by default, specifying an unencrypted password.

  The failover key shared secret shows as ***** in show running-config output; this obscured key is not copyable.

  If you do not configure failover and state link encryption, failover communication, including any passwords or keys in the configuration that are sent during command replication, will be in clear text.

**Step 9** Create failover group 1:

```bash
failover group 1
```

By default, this group is assigned to the primary unit. Typically, you assign group 1 to the primary unit, and group 2 to the secondary unit. If you want a non-standard configuration, you can specify different unit preferences if desired using the primary or secondary subcommands.

**Step 10** Create failover group 2 and assigns it to the secondary unit:

```bash
failover group 2 secondary
```

**Step 11** Enter the context configuration mode for a given context, and assign the context to a failover group:

```bash
context name
  join-failover-group {1 | 2}
```

Example:

```bash
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

Repeat this command for each context.

Any unassigned contexts are automatically assigned to failover group 1. The admin context is always a member of failover group 1; you cannot assign it to group 2.

**Step 12** Enable failover:

```bash
failover
```

**Step 13** Save the system configuration to flash memory:
Examples

The following example configures the failover parameters for the primary unit:

```plaintext
write memory

failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover group 1
failover group 2
  secondary
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
```

Configure the Secondary Unit for Active/Active Failover

The only configuration required on the secondary unit is for the failover link. The secondary unit requires these commands to communicate initially with the primary unit. After the primary unit sends its configuration to the secondary unit, the only permanent difference between the two configurations is the `failover lan unit` command, which identifies each unit as primary or secondary.

Before You Begin

- Enable multiple context mode according to [Enable or Disable Multiple Context Mode, page 6-15](#).
- Do not configure a `nameif` for the failover and state links.
- Complete this procedure in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.

Procedure

**Step 1**

Re-enter the exact same commands as on the primary unit except for the `failover lan unit primary` command. You can optionally replace it with the `failover lan unit secondary` command, but it is not necessary because `secondary` is the default setting. You also do not need to enter the `failover group` and `join-failover-group` commands, as they are replicated from the primary unit. See [Configure the Primary Unit for Active/Active Failover, page 7-29](#).

For example:

```plaintext
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces

ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2

ciscoasa(config)# interface gigabitethernet 0/3
  no shutdown

ciscoasa(config)# failover link statelink gigabitethernet0/4
```
Configure Optional Failover Parameters

You can customize failover settings as desired.

- Configure Failover Criteria, HTTP Replication, Group Preemption, Standby Configuration Lock, and MAC Addresses, page 7-34
- Configure Interface Monitoring, page 7-37
- Configure Support for Asymmetrically Routed Packets (Active/Active Mode), page 7-38

Configure Failover Criteria, HTTP Replication, Group Preemption, Standby Configuration Lock, and MAC Addresses

See Defaults for Failover, page 7-25 for the default settings for many parameters that you can change in this section. For Active/Active mode, you set most criteria per failover group.

Before You Begin
Configure these settings in the system execution space in multiple context mode.

Procedure

Step 1 Change the unit poll and hold times:
In Active/Active mode, you set this rate for the system; you cannot set this rate per failover group.
You cannot enter a holdtime value that is less than 3 times the unit poll time. With a faster poll time, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchover when the network is temporarily congested.
If a unit does not hear hello packet on the failover communication interface for one polling period, additional testing occurs through the remaining interfaces. If there is still no response from the peer unit during the hold time, the unit is considered failed and, if the failed unit is the active unit, the standby unit takes over as the active unit.

```
failover polltime [unit] [msec] poll_time [holdtime [msec] time]
```
Chapter 7  Failover for High Availability

Configure Optional Failover Parameters

Example:
```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

Step 2  Set the HTTP replication rate in connections per second:

Set the rate between 8341 and 50000. The default is 50000. In Active/Active mode, you set this rate for the system; you cannot set this rate per failover group.

```
failover replication rate conns
```

Example:
```
ciscoasa(config)# failover replication rate 20000
```

Step 3  Disable the ability to make any configuration changes directly on the standby unit or context:

By default, configurations on the standby unit/context are allowed with a warning message.

```
failover standby config-lock
```

Step 4  (Active/Active mode only) Specify the failover group you want to customize:

```
failover group (1 | 2)
```

Example:
```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

Step 5  (Active/Active mode only) Configure failover group preemption for failover group 1:

```
preempt [delay]
```

Example:
```
ciscoasa(config-fover-group)# preempt 1200
```

If one unit boots before the other, then both failover groups become active on that unit, despite the primary or secondary setting. This command causes the failover group to become active on the designated unit automatically when that unit becomes available.

You can enter an optional \texttt{delay} value, which specifies the number of seconds the failover group remains active on the current unit before automatically becoming active on the designated unit. Valid values are from 1 to 1200.

If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the unit on which the failover group is currently active.

Step 6  Enable HTTP state replication:

- For Active/Standby mode:
  ```
  failover replication http
  ```

- For Active/Active mode:
  ```
  replication http
  ```

To allow HTTP connections to be included in the state information replication, you need to enable HTTP replication. Because HTTP connections are typically short-lived, and because HTTP clients typically retry failed connection attempts, HTTP connections are not automatically included in the replicated state information.

Step 7  Set the threshold for failover when interfaces fail:

- For Active/Standby mode:
**Chapter 7**  
**Failover for High Availability**

Configure Optional Failover Parameters

**failover interface-policy num[%]**

Example:
```
ciscoasa (config)# failover interface-policy 20%
```

- For Active/Active mode:
  **interface-policy num[%]**

Example:
```
ciscoasa(config-fover-group)# interface-policy 20%
```

By default, one interface failure causes failover.

When specifying a specific number of interfaces, the `num` argument can be from 1 to 250.

When specifying a percentage of interfaces, the `num` argument can be from 1 to 100.

**Step 8** Change the interface poll and hold times:

- For Active/Standby mode:
  **failover polltime interface [msec] time [holdtime time]**

Example:
```
ciscoasa(config)# failover polltime interface msec 500 holdtime 5
```

- For Active/Active mode:
  **polltime interface [msec] time [holdtime time]**

Example:
```
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
```

Valid values for poll time are from 1 to 15 seconds or, if the optional `msec` keyword is used, from 500 to 999 milliseconds. The hold time determines how long it takes from the time a hello packet is missed to when the interface is marked as failed. Valid values for the hold time are from 5 to 75 seconds. You cannot enter a hold time that is less than 5 times the poll time.

If the interface link is down, interface testing is not conducted and the standby unit could become active in just one interface polling period if the number of failed interfaces meets or exceeds the configured failover criteria.

**Step 9** Configure the virtual MAC address for an interface:

- For Active/Standby mode:
  **failover mac address phy_if active_mac standby_mac**

Example:
```
ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

- For Active/Active mode:
  **mac address phy_if active_mac standby_mac**

Example:
```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

The `phy_if` argument is the physical name of the interface, such as gigabitethernet0/1.
The `active_mac` and `standby_mac` arguments are MAC addresses in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

The `active_mac` address is associated with the active IP address for the interface, and the `standby_mac` is associated with the standby IP address for the interface.

You can also set the MAC address using other commands or methods, but we recommend using only one method. If you set the MAC address using multiple methods, the MAC address used depends on many variables, and might not be predictable.

Use the `show interface` command to display the MAC address used by an interface.

**Step 10**

(Active/Active mode only) Repeat this procedure for the other failover group, if desired.

**Step 11**

**Step 12**

**Step 13**

**Step 14**

a.

b.

c.

### Configure Interface Monitoring

By default, monitoring is enabled on all physical interfaces, or for the ASASM, all VLAN interfaces, and on any hardware modules installed on the ASA. You might want to exclude interfaces attached to less critical networks from affecting your failover policy.

**Before You Begin**

- You can monitor up to 250 interfaces on a unit (across all contexts in multiple context mode).
- In multiple context mode, configure interfaces within each context.

**Procedure**

**Step 1**

Enable or disable health monitoring for an interface:

```plaintext
[no] monitor-interface {if_name | service-module}
```

Example:

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```
If you do not want a hardware module failure, such as the ASA FirePOWER module, to trigger failover, you can disable module monitoring using the `no monitor-interface service-module` command.

---

**Configure Support for Asymmetrically Routed Packets (Active/Active Mode)**

When running in Active/Active failover, a unit may receive a return packet for a connection that originated through its peer unit. Because the ASA that receives the packet does not have any connection information for the packet, the packet is dropped. This drop most commonly occurs when the two ASAs in an Active/Active failover pair are connected to different service providers and the outbound connection does not use a NAT address.

You can prevent the return packets from being dropped by allowing asymmetrically routed packets. To do so, you assign the similar interfaces on each ASA to the same ASR group. For example, both ASAs connect to the inside network on the inside interface, but connect to separate ISPs on the outside interface. On the primary unit, assign the active context outside interface to ASR group 1; on the secondary unit, assign the active context outside interface to the same ASR group 1. When the primary unit outside interface receives a packet for which it has no session information, it checks the session information for the other interfaces in standby contexts that are in the same group; in this case, ASR group 1. If it does not find a match, the packet is dropped. If it finds a match, then one of the following actions occurs:

- If the incoming traffic originated on a peer unit, some or all of the layer 2 header is rewritten and the packet is redirected to the other unit. This redirection continues as long as the session is active.
- If the incoming traffic originated on a different interface on the same unit, some or all of the layer 2 header is rewritten and the packet is reinjected into the stream.

---

**Note**

This feature does not provide asymmetric routing; it restores asymmetrically routed packets to the correct interface.
Figure 7-13 shows an example of an asymmetrically routed packet.

**Figure 7-13  ASR Example**

1. An outbound session passes through the ASA with the active SecAppA context. It exits interface outsideISP-A (192.168.1.1).

2. Because of asymmetric routing configured somewhere upstream, the return traffic comes back through the interface outsideISP-B (192.168.2.2) on the ASA with the active SecAppB context.

3. Normally the return traffic would be dropped because there is no session information for the traffic on interface 192.168.2.2. However, the interface is configured as part of ASR group 1. The unit looks for the session on any other interface configured with the same ASR group ID.

4. The session information is found on interface outsideISP-A (192.168.1.2), which is in the standby state on the unit with SecAppB. Stateful Failover replicated the session information from SecAppA to SecAppB.

5. Instead of being dropped, the layer 2 header is rewritten with information for interface 192.168.1.1 and the traffic is redirected out of the interface 192.168.1.2, where it can then return through the interface on the unit from which it originated (192.168.1.1 on SecAppA). This forwarding continues as needed until the session ends.

**Before You Begin**

- Stateful Failover—Passes state information for sessions on interfaces in the active failover group to the standby failover group.

- Replication HTTP—HTTP session state information is not passed to the standby failover group, and therefore is not present on the standby interface. For the ASA to be able to re-route asymmetrically routed HTTP packets, you need to replicate the HTTP state information.

- Perform this procedure within each active context on the primary and secondary units.
Configure Optional Failover Parameters

You cannot configure both ASR groups and traffic zones within a context. If you configure a zone in a context, none of the context interfaces can be part of an ASR group.

Procedure

**Step 1** On the primary unit, specify the interface for which you want to allow asymmetrically routed packets:

```
interface phy_if
```

Example:

```
primary/admin(config)# interface gigabitethernet 0/0
```

**Step 2** Set the ASR group number for the interface:

```
asr-group num
```

Example:

```
primary/admin(config-ifc)# asr-group 1
```

Valid values for `num` range from 1 to 32.

**Step 3** On the secondary unit, specify the similar interface for which you want to allow asymmetrically routed packets:

```
interface phy_if
```

Example:

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

**Step 4** Set the ASR group number for the interface to match the primary unit interface:

```
asr-group num
```

Example:

```
secondary/ctx1(config-ifc)# asr-group 1
```

Examples

The two units have the following configuration (configurations show only the relevant commands). The device labeled SecAppA in the diagram is the primary unit in the failover pair.

### Example 7-1 Primary Unit System Configuration

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
```
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
  context admin
    allocate-interface GigabitEthernet0/2
    allocate-interface GigabitEthernet0/3
    config-url flash:/admin.cfg
    join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2

Example 7-2  SecAppA Context Configuration

interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
  monitor-interface outside

Example 7-3  SecAppB Context Configuration

interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11

Manage Failover

This section describes how to manage failover units after you enable failover, including how to change the failover setup and how to force failover from one unit to another.

- Force Failover, page 7-42
- Disable Failover, page 7-42
- Restore a Failed Unit, page 7-43
- Re-Sync the Configuration, page 7-44
- Test the Failover Functionality, page 7-44
- Remote Command Execution, page 7-45
Force Failover

To force the standby unit to become active, perform the following procedure.

Before You Begin
In multiple context mode, perform this procedure in the System execution space.

Procedure

Step 1  Force a failover when entered on the standby unit. The standby unit becomes the active unit.
If you specify the \texttt{group group\_id}, then this command forces a failover when entered on the standby unit for the specified Active/Active failover group. The standby unit becomes the active unit for the failover group.

- For Active/Standby mode on the standby unit:
  \texttt{failover active}

- For Active/Active mode on the standby unit:
  \texttt{failover active [group group\_id]}

Example:

\begin{verbatim}
standby# failover active group 1
\end{verbatim}

Step 2  Force a failover when entered on the active unit. The active unit becomes the standby unit.
If you specify the \texttt{group group\_id}, then this command forces a failover when entered on the active unit for the specified failover group. The active unit becomes the standby unit for the failover group.

- For Active/Standby mode on the active unit:
  \texttt{no failover active}

- For Active/Active mode on the active unit:
  \texttt{no failover active [group group\_id]}

Example:

\begin{verbatim}
active# no failover active group 1
\end{verbatim}

Disable Failover

Disabling failover on one or both units causes the active and standby state of each unit to be maintained until you reload. For an Active/Active failover pair, the failover groups remain in the active state on whichever unit they are active, no matter which unit they are configured to prefer.

See the following characteristics when you disable failover:

- The standby unit/context remains in standby mode so that both units do not start passing traffic (this is called a pseudo-standby state).
- The standby unit/context continues to use its standby IP addresses even though it is no longer connected to an active unit/context.
The standby unit/context continues to listen for a connection on the failover link. If failover is re-enabled on the active unit/context, then the standby unit/context resumes ordinary standby status after re-synchronizing the rest of its configuration.

To truly disable failover, save the no failover configuration to the startup configuration, and then reload.

**Before You Begin**
In multiple context mode, perform this procedure in the system execution space.

**Procedure**

**Step 1**
Disable failover:

```
no failover
```

**Step 2**
To completely disable failover, save the configuration and reload:

```
write memory
reload
```

**Step 3**

### Restore a Failed Unit

To restore a failed unit to an unfailed state, perform the following procedure.

**Before You Begin**
In multiple context mode, perform this procedure in the System execution space.

**Procedure**

**Step 1**
Restore a failed unit to an unfailed state:

- For Active/Standby mode:

  ```
  failover reset
  ```

- For Active/Active mode:

  ```
  failover reset [group group_id]
  ```

Example:

```
ciscoasa(config)# failover reset group 1
```

Restoring a failed unit to an unfailed state does not automatically make it active; restored units remain in the standby state until made active by failover (forced or natural). An exception is a failover group (Active/Active mode only) configured with failover preemption. If previously active, a failover group becomes active if it is configured with preemption and if the unit on which it failed is the preferred unit.

If you specify the **group group_id**, this command restores a failed Active/Active failover group to an unfailed state.
Re-Sync the Configuration

If you enter the `write standby` command on the active unit, the standby unit clears its running configuration (except for the failover commands used to communicate with the active unit), and the active unit sends its entire configuration to the standby unit.

For multiple context mode, when you enter the `write standby` command in the system execution space, all contexts are replicated. If you enter the `write standby` command within a context, the command replicates only the context configuration.

Replicated commands are stored in the running configuration.

Test the Failover Functionality

To test failover functionality, perform the following procedure.

Procedure

**Step 1** Test that your active unit is passing traffic as expected by using FTP (for example) to send a file between hosts on different interfaces.

**Step 2** Force a failover by entering the following command on the active unit:

- **Active/Standby mode:**
  ```
  ciscoasa(config)# no failover active
  ```

- **Active/Active mode:**
  ```
  ciscoasa(config)# no failover active group group_id
  ```

**Step 3** Use FTP to send another file between the same two hosts.

**Step 4** If the test was not successful, enter the `show failover` command to check the failover status.

**Step 5** When you are finished, you can restore the unit to active status by enter the following command on the newly active unit:

- **Active/Standby mode:**
  ```
  ciscoasa(config)# no failover active
  ```

- **Active/Active mode:**
  ```
  ciscoasa(config)# failover active group group_id
  ```

**Note**

When an ASA interface goes down, for failover it is still considered to be a unit issue. If the ASA detects that an interface is down, failover occurs immediately, without waiting for the interface holdtime. The interface holdtime is only useful when the ASA considers its status to be OK, although it is not receiving hello packets from the peer. To simulate interface holdtime, shut down the VLAN on the switch to prevent peers from receiving hello packets from each other.
Remote Command Execution

Remote command execution lets you send commands entered at the command line to a specific failover peer.

- Send a Command, page 7-45
- Change Command Modes, page 7-45
- Security Considerations, page 7-46
- Limitations of Remote Command Execution, page 7-46

Send a Command

Because configuration commands are replicated from the active unit or context to the standby unit or context, you can use the `failover exec` command to enter configuration commands on the correct unit, no matter which unit you are logged in to. For example, if you are logged in to the standby unit, you can use the `failover exec active` command to send configuration changes to the active unit. Those changes are then replicated to the standby unit. Do not use the `failover exec` command to send configuration commands to the standby unit or context; those configuration changes are not replicated to the active unit and the two configurations will no longer be synchronized.

Output from configuration, exec, and `show` commands is displayed in the current terminal session, so you can use the `failover exec` command to issue `show` commands on a peer unit and view the results in the current terminal.

You must have sufficient privileges to execute a command on the local unit to execute the command on the peer unit.

**Procedure**

**Step 1** If you are in multiple context mode, use the `changeto context name` command to change to the context you want to configure. You cannot change contexts on the failover peer with the `failover exec` command.

**Step 2** Use the following command to send commands to the specified failover unit:

```
ciscoasa(config)# failover exec {active | mate | standby}
```

Use the `active` or `standby` keyword to cause the command to be executed on the specified unit, even if that unit is the current unit. Use the `mate` keyword to cause the command to be executed on the failover peer.

Commands that cause a command mode change do not change the prompt for the current session. You must use the `show failover exec` command to display the command mode the command is executed in. See Change Command Modes, page 7-45 for more information.

Change Command Modes

The `failover exec` command maintains a command mode state that is separate from the command mode of your terminal session. By default, the `failover exec` command mode starts in global configuration mode for the specified device. You can change that command mode by sending the appropriate command (such as the `interface` command) using the `failover exec` command. The session prompt does not change when you change modes using `failover exec`. 
For example, if you are logged in to global configuration mode of the active unit of a failover pair, and you use the `failover exec active` command to change to interface configuration mode, the terminal prompt remains in global configuration mode, but commands entered using `failover exec` are entered in interface configuration mode.

The following examples show the difference between the terminal session mode and the `failover exec` command mode. In the example, the administrator changes the `failover exec` mode on the active unit to interface configuration mode for the interface GigabitEthernet0/1. After that, all commands entered using `failover exec active` are sent to interface configuration mode for interface GigabitEthernet0/1. The administrator then uses failover exec active to assign an IP address to that interface. Although the prompt indicates global configuration mode, the `failover exec active` mode is in interface configuration mode.

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
```

Changing commands modes for your current session to the device does not affect the command mode used by the `failover exec` command. For example, if you are in interface configuration mode on the active unit, and you have not changed the `failover exec` command mode, the following command would be executed in global configuration mode. The result would be that your session to the device remains in interface configuration mode, while commands entered using `failover exec active` are sent to router configuration mode for the specified routing process.

```
ciscoasa(config-if)# failover exec active router ospf 100
```

Use the `show failover exec` command to display the command mode on the specified device in which commands sent with the `failover exec` command are executed. The `show failover exec` command takes the same keywords as the `failover exec` command: `active`, `mate`, or `standby`. The `failover exec` mode for each device is tracked separately.

For example, the following is sample output from the `show failover exec` command entered on the standby unit:

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
```

```
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode
```

```
ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode
```

```
ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

Security Considerations

The `failover exec` command uses the failover link to send commands to and receive the output of the command execution from the peer unit. You should enable encryption on the failover link to prevent eavesdropping or man-in-the-middle attacks.

Limitations of Remote Command Execution

When you use remote commands you face the following limitations:

- If you upgrade one unit using the zero-downtime upgrade procedure and not the other, both units must be running software that supports the `failover exec` command for the command to work.
Chapter 7  Failover for High Availability

Monitoring Failover

- Command completion and context help is not available for the commands in the cmd_string argument.
- In multiple context mode, you can only send commands to the peer context on the peer unit. To send commands to a different context, you must first change to that context on the unit to which you are logged in.
- You cannot use the following commands with the failover exec command:
  - changeto
  - debug (undebug)
- If the standby unit is in the failed state, it can still receive commands from the failover exec command if the failure is due to a service card failure; otherwise, the remote command execution will fail.
- You cannot use the failover exec command to switch from privileged EXEC mode to global configuration mode on the failover peer. For example, if the current unit is in privileged EXEC mode, and you enter failover exec mate configure terminal, the show failover exec mate output will show that the failover exec session is in global configuration mode. However, entering configuration commands for the peer unit using failover exec will fail until you enter global configuration mode on the current unit.
- You cannot enter recursive failover exec commands, such as failover exec mate failover exec mate command.
- Commands that require user input or confirmation must use the /nonconfirm option.

Monitoring Failover Messages

Failover Messages

- Failover Syslog Messages, page 7-47
- Failover Debug Messages, page 7-48
- SNMP Failover Traps, page 7-48

Failover Syslog Messages

When a failover occurs, both ASAs send out system messages.

- Failover Syslog Messages, page 7-47
- Failover Debug Messages, page 7-48
- SNMP Failover Traps, page 7-48

Note

During a fail over, failover logically shuts down and then bring up interfaces, generating syslog messages 411001 and 411002. This is normal activity.
Failover Debug Messages

To see debug messages, enter the `debug failover` command. See the command reference for more information.

**Note** Because debugging output is assigned high priority in the CPU process, it can drastically affect system performance. For this reason, use the `debug failover` commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC.

SNMP Failover Traps

To receive SNMP syslog traps for failover, configure the SNMP agent to send SNMP traps to SNMP management stations, define a syslog host, and compile the Cisco syslog MIB into your SNMP management station. See Chapter 40, “SNMP” for more information.

Monitoring Failover Status

To monitor failover status, enter one of the following commands:

- `show failover`
  Displays information about the failover state of the unit.
- `show failover group`
  Displays information about the failover state of the failover group. The information displayed is similar to that of the `show failover` command but limited to the specified group.
- `show monitor-interface`
  Displays information about the monitored interface.
- `show running-config failover`
  Displays the failover commands in the running configuration.

History for Failover

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active/Standby failover</td>
<td>7.0(1)</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Active/Active failover</td>
<td>7.0(1)</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
| Support for a hex value for the failover key | 7.0(4)   | You can now specify a hex value for failover link encryption.  
|                               |          | We modified the following command: `failover key hex`.    |
Support for the master passphrase for the failover key  8.3(1)

The failover key now supports the master passphrase, which encrypts the shared key in the running and startup configuration. If you are copying the shared secret from one ASA to another, for example from the `more system:running-config` command, you can successfully copy and paste the encrypted shared key.

**Note** The `failover key` shared secret shows as ***** in `show running-config` output; this obscured key is not copyable.

We modified the following command: `failover key [0 | 8].`

IPv6 support for failover added.  8.2(2)

We modified the following commands: `failover interface ip`, `show failover`, `ipv6 address`, `show monitor-interface`.

Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications  9.1(2)

Instead of using the proprietary encryption for the failover key (the `failover key` command), you can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption.

**Note** Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license.

We introduced or modified the following commands: `failover ipsec pre-shared-key`, `show vpn-sessiondb`.

Disable health monitoring of a hardware module  9.3(1)

By default, the ASA monitors the health of an installed hardware module such as the ASA FirePOWER module. If you do not want a hardware module failure to trigger failover, you can disable module monitoring.

We modified the following command: `monitor-interface service-module`.

Lock configuration changes on the standby unit or standby context in a failover pair  9.3(2)

You can now lock configuration changes on the standby unit (Active/Standby failover) or the standby context (Active/Active failover) so you cannot make changes on the standby unit outside normal configuration syncing.

We introduced the following command: `failover standby config-lock`.

### Table 7-4 History for Failover

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for the master passphrase for the failover key</td>
<td>8.3(1)</td>
<td>The failover key now supports the master passphrase, which encrypts the shared key in the running and startup configuration. If you are copying the shared secret from one ASA to another, for example from the <code>more system:running-config</code> command, you can successfully copy and paste the encrypted shared key. <strong>Note</strong> The <code>failover key</code> shared secret shows as ***** in <code>show running-config</code> output; this obscured key is not copyable. We modified the following command: `failover key [0</td>
</tr>
<tr>
<td>IPv6 support for failover added.</td>
<td>8.2(2)</td>
<td>We modified the following commands: <code>failover interface ip</code>, <code>show failover</code>, <code>ipv6 address</code>, <code>show monitor-interface</code>.</td>
</tr>
<tr>
<td>Support for IPsec LAN-to-LAN tunnels to encrypt failover and state link communications</td>
<td>9.1(2)</td>
<td>Instead of using the proprietary encryption for the failover key (the <code>failover key</code> command), you can now use an IPsec LAN-to-LAN tunnel for failover and state link encryption. <strong>Note</strong> Failover LAN-to-LAN tunnels do not count against the IPsec (Other VPN) license. We introduced or modified the following commands: <code>failover ipsec pre-shared-key</code>, <code>show vpn-sessiondb</code>.</td>
</tr>
<tr>
<td>Disable health monitoring of a hardware module</td>
<td>9.3(1)</td>
<td>By default, the ASA monitors the health of an installed hardware module such as the ASA FirePOWER module. If you do not want a hardware module failure to trigger failover, you can disable module monitoring. We modified the following command: <code>monitor-interface service-module</code></td>
</tr>
<tr>
<td>Lock configuration changes on the standby unit or standby context in a failover pair</td>
<td>9.3(2)</td>
<td>You can now lock configuration changes on the standby unit (Active/Standby failover) or the standby context (Active/Active failover) so you cannot make changes on the standby unit outside normal configuration syncing. We introduced the following command: <code>failover standby config-lock</code>.</td>
</tr>
</tbody>
</table>
ASA Cluster

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.

**Note**

Some features are not supported when using clustering. See [Unsupported Features with Clustering](#), page 8-25.

- About ASA Clustering, page 8-1
- Licensing for ASA Clustering, page 8-32
- Prerequisites for ASA Clustering, page 8-32
- Guidelines for ASA Clustering, page 8-33
- Defaults for ASA Clustering, page 8-37
- Configure ASA Clustering, page 8-37
- Manage ASA Cluster Members, page 8-54
- Monitoring the ASA Cluster, page 8-59
- Examples for ASA Clustering, page 8-64
- History for ASA Clustering, page 8-76

### About ASA Clustering

This section describes the clustering architecture and how it works.

- How the ASA Cluster Fits into Your Network, page 8-2
- Performance Scaling Factor, page 8-2
- Cluster Members, page 8-3
- Cluster Interfaces, page 8-4
- Cluster Control Link, page 8-5
- High Availability Within the ASA Cluster, page 8-8
- Configuration Replication, page 8-11
- ASA Cluster Management, page 8-11
How the ASA Cluster Fits into Your Network

The cluster consists of multiple ASAs acting as a single unit. To act as a cluster, the ASAs need the following infrastructure:

- Isolated, high-speed backplane network for intra-cluster communication, known as the cluster control link.
- Management access to each ASA for configuration and monitoring.

When you place the cluster in your network, the upstream and downstream routers need to be able to load-balance the data coming to and from the cluster using one of the following methods:

- Spanned EtherChannel (Recommended)—Interfaces on multiple members of the cluster are grouped into a single EtherChannel; the EtherChannel performs load balancing between units.
- Policy-Based Routing (Routed firewall mode only)—The upstream and downstream routers perform load balancing between units using route maps and ACLs.
- Equal-Cost Multi-Path Routing (Routed firewall mode only)—The upstream and downstream routers perform load balancing between units using equal cost static or dynamic routes.

Related Topics

- Licensing for ASA Clustering, page 8-32
- Cluster Control Link, page 8-5
- ASA Cluster Management, page 8-11
- Spanned EtherChannel (Recommended), page 8-13
- Policy-Based Routing (Routed Firewall Mode Only), page 8-17
- Equal-Cost Multi-Path Routing (Routed Firewall Mode Only), page 8-18

Performance Scaling Factor

When you combine multiple units into a cluster, you can expect a performance of approximately:

- 70% of the combined throughput
- 60% of maximum connections
- 50% of connections per second

For example, for throughput, the ASA 5585-X with SSP-40 can handle approximately 10 Gbps of real world firewall traffic when running alone. For a cluster of 8 units, the maximum combined throughput will be approximately 70% of 80 Gbps (8 units x 10 Gbps): 56 Gbps.
Cluster Members

Cluster members work together to accomplish the sharing of the security policy and traffic flows. This section describes the nature of each member role.

- Bootstrap Configuration, page 8-3
- Master and Slave Unit Roles, page 8-3
- Master Unit Election, page 8-3

Bootstrap Configuration

On each device, you configure a minimal bootstrap configuration including the cluster name, cluster control link interface, and other cluster settings. The first unit on which you enable clustering typically becomes the master unit. When you enable clustering on subsequent units, they join the cluster as slaves.

Master and Slave Unit Roles

One member of the cluster is the master unit. The master unit is determined by the priority setting in the bootstrap configuration; the priority is set between 1 and 100, where 1 is the highest priority. All other members are slave units. Typically, when you first create a cluster, the first unit you add becomes the master unit simply because it is the only unit in the cluster so far.

You must perform all configuration (aside from the bootstrap configuration) on the master unit only; the configuration is then replicated to the slave units. In the case of physical assets, such as interfaces, the configuration of the master unit is mirrored on all slave units. For example, if you configure GigabitEthernet 0/1 as the inside interface and GigabitEthernet 0/0 as the outside interface, then these interfaces are also used on the slave units as inside and outside interfaces.

Some features do not scale in a cluster, and the master unit handles all traffic for those features.

Related Topics
- Centralized Features for Clustering, page 8-26

Master Unit Election

Members of the cluster communicate over the cluster control link to elect a master unit as follows:

1. When you enable clustering for a unit (or when it first starts up with clustering already enabled), it broadcasts an election request every 3 seconds.
2. Any other units with a higher priority respond to the election request; the priority is set between 1 and 100, where 1 is the highest priority.
3. If after 45 seconds, a unit does not receive a response from another unit with a higher priority, then it becomes master.

Note If multiple units tie for the highest priority, the cluster unit name and then the serial number is used to determine the master.

4. If a unit later joins the cluster with a higher priority, it does not automatically become the master unit; the existing master unit always remains as the master unless it stops responding, at which point a new master unit is elected.
Note
You can manually force a unit to become the master. For centralized features, if you force a master unit change, then all connections are dropped, and you have to re-establish the connections on the new master unit.

Related Topics
- Centralized Features for Clustering, page 8-26

Cluster Interfaces

You can configure data interfaces as either Spanned EtherChannels or as Individual interfaces. All data interfaces in the cluster must be one type only.

Spanned EtherChannel (Recommended)

You can group one or more interfaces per unit into an EtherChannel that spans all units in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel. A Spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the bridge group, not to the interface. The EtherChannel inherently provides load balancing as part of basic operation.
Individual Interfaces (Routed Firewall Mode Only)

Individual interfaces are normal routed interfaces, each with their own Local IP address. Because interface configuration must be configured only on the master unit, the interface configuration lets you set a pool of IP addresses to be used for a given interface on the cluster members, including one for the master. The Main cluster IP address is a fixed address for the cluster that always belongs to the current master unit. The Main cluster IP address is a secondary IP address for the master unit; the Local IP address is always the primary address for routing. The Main cluster IP address provides consistent management access to an address; when a master unit changes, the Main cluster IP address moves to the new master unit, so management of the cluster continues seamlessly. Load balancing, however, must be configured separately on the upstream switch in this case.

Note
We recommend Spanned EtherChannels instead of Individual interfaces because Individual interfaces rely on routing protocols to load-balance traffic, and routing protocols often have slow convergence during a link failure.

Cluster Control Link

Each unit must dedicate at least one hardware interface as the cluster control link.

- Cluster Control Link Traffic Overview, page 8-6
Cluster Control Link Traffic Overview

Cluster control link traffic includes both control and data traffic. Control traffic includes:

- Master election.
- Configuration replication.
- Health monitoring.

Data traffic includes:

- State replication.
- Connection ownership queries and data packet forwarding.

Related Topics

- Cluster Members, page 8-3
- Configuration Replication, page 8-11
- Unit Health Monitoring, page 8-9
- Data Path Connection State Replication, page 8-10
- Rebalancing New TCP Connections Across the Cluster, page 8-24

Cluster Control Link Interfaces and Network

You can use any data interface(s) for the cluster control link, with the following exceptions:

- You cannot use a VLAN subinterface as the cluster control link.
- You cannot use a Management x/x interface as the cluster control link, either alone or as an EtherChannel.
- For the ASA 5585-X with an ASA IPS module, you cannot use the module interfaces for the cluster control link; you can, however, use interfaces on the ASA 5585-X Network Module.

You can use an EtherChannel or redundant interface.

For the ASA 5585-X with SSP-10 and SSP-20, which include two Ten Gigabit Ethernet interfaces, we recommend using one interface for the cluster control link, and the other for data (you can use subinterfaces for data). Although this setup does not accommodate redundancy for the cluster control link, it does satisfy the need to size the cluster control link to match the size of the data interfaces.

Each cluster control link has an IP address on the same subnet. This subnet should be isolated from all other traffic, and should include only the ASA cluster control link interfaces.
For a 2-member cluster, do not directly-connect the cluster control link from one ASA to the other ASA. If you directly connect the interfaces, then when one unit fails, the cluster control link fails, and thus the remaining healthy unit fails. If you connect the cluster control link through a switch, then the cluster control link remains up for the healthy unit.

Related Topics
- Cluster Control Link Redundancy, page 8-7
- Size the Cluster Control Link, page 8-7

Size the Cluster Control Link

You should size the cluster control link to match the expected throughput of each member. For example, if you have the ASA 5585-X with SSP-60, which can pass 14 Gbps per unit maximum in a cluster, then you should also assign interfaces to the cluster control link that can pass at least 14 Gbps. In this case, you could use 2 Ten Gigabit Ethernet interfaces in an EtherChannel for the cluster control link, and use the rest of the interfaces as desired for data links.

Cluster control link traffic is comprised mainly of state update and forwarded packets. The amount of traffic at any given time on the cluster control link varies. For example state updates could consume up to 10% of the through traffic amount if through traffic consists exclusively of short-lived TCP connections. The amount of forwarded traffic depends on the load-balancing efficacy or whether there is a lot of traffic for centralized features. For example:

- NAT results in poor load balancing of connections, and the need to rebalance all returning traffic to the correct units.
- AAA for network access is a centralized feature, so all traffic is forwarded to the master unit.
- When membership changes, the cluster needs to rebalance a large number of connections, thus temporarily using a large amount of cluster control link bandwidth.

A higher-bandwidth cluster control link helps the cluster to converge faster when there are membership changes and prevents throughput bottlenecks.

Note
If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

Related Topics
- Inter-Site Clustering, page 8-18.

Cluster Control Link Redundancy

We recommend using an EtherChannel for the cluster control link, so that you can pass traffic on multiple links in the EtherChannel while still achieving redundancy.

The following diagram shows how to use an EtherChannel as a cluster control link in a Virtual Switching System (VSS) or Virtual Port Channel (vPC) environment. All links in the EtherChannel are active. When the switch is part of a VSS or vPC, then you can connect ASA interfaces within the same EtherChannel to separate switches in the VSS or vPC. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch. Note that this EtherChannel is device-local, not a Spanned EtherChannel.
Cluster Control Link Reliability

To ensure cluster control link functionality, be sure the round-trip time (RTT) between units is less than 20 ms. This maximum latency enhances compatibility with cluster members installed at different geographical sites. To check your latency, perform a ping on the cluster control link between units.

The cluster control link must be reliable, with no out-of-order or dropped packets; for example, for inter-site deployment, you should use a dedicated link.

Cluster Control Link Failure

If the cluster control link line protocol goes down for a unit, then clustering is disabled; data interfaces are shut down. After you fix the cluster control link, you must manually rejoin the cluster by re-enabling clustering.

Note

When an ASA becomes inactive, all data interfaces are shut down; only the management-only interface can send and receive traffic. The management interface remains up using the IP address the unit received from the cluster IP pool. However if you reload, and the unit is still inactive in the cluster, the management interface is not accessible (because it then uses the Main IP address, which is the same as the master unit). You must use the console port for any further configuration.

Related Topics
Rejoining the Cluster, page 8-10

High Availability Within the ASA Cluster

ASA Clustering provides high availability by monitoring unit and interface health and by replicating connection states between units.

- Unit Health Monitoring, page 8-9
- Interface Monitoring, page 8-9
- Unit or Interface Failure, page 8-9
- Data Path Connection State Replication, page 8-10
Unit Health Monitoring

The master unit monitors every slave unit by sending keepalive messages over the cluster control link periodically (the period is configurable). Each slave unit monitors the master unit using the same mechanism.

Interface Monitoring

Each unit monitors the link status of all hardware interfaces in use, and reports status changes to the master unit.

- Spanned EtherChannel—Uses cluster Link Aggregation Control Protocol (cLACP). Each unit monitors the link status and the cLACP protocol messages to determine if the port is still active in the EtherChannel. The status is reported to the master unit.
- Individual interfaces (Routed mode only)—Each unit self-monitors its interfaces and reports interface status to the master unit.

Unit or Interface Failure

When health monitoring is enabled, a unit is removed from the cluster if it fails or if its interfaces fail. If all physical ports for a given logical interface fail on a particular unit, but there are active ports under the same logical interface on other units, then the unit is removed from the cluster. The amount of time before the ASA removes a member from the cluster depends on the type of interface and whether the unit is an established member or is joining the cluster. For EtherChannels (spanned or not), if the interface is down on an established member, then the ASA removes the member after 9 seconds. The ASA does not monitor interfaces for the first 90 seconds that a unit joins the cluster. Interface status changes during this time will not cause the ASA to be removed from the cluster. For non-EtherChannels, the unit is removed after 500 ms, regardless of the member state.

When a unit in the cluster fails, the connections hosted by that unit are seamlessly transferred to other units; state information for traffic flows is shared over the control cluster link.

If the master unit fails, then another member of the cluster with the highest priority (lowest number) becomes the master.

The ASA automatically tries to rejoin the cluster.

Note

When an ASA becomes inactive and fails to automatically rejoin the cluster, all data interfaces are shut down; only the management-only interface can send and receive traffic. The management interface remains up using the IP address the unit received from the cluster IP pool. However if you reload, and the unit is still inactive in the cluster, the management interface is not accessible (because it then uses the Main IP address, which is the same as the master unit). You must use the console port for any further configuration.

Related Topics

Rejoining the Cluster, page 8-10
Rejoining the Cluster

After a cluster member is removed from the cluster, how it can rejoin the cluster depends on why it was removed:

- Failed cluster control link—After you resolve the problem with the cluster control link, you must manually rejoin the cluster by re-enabling clustering at the console port by entering `cluster name`, and then `enable`.

- Failed data interface—The ASA automatically tries to rejoin at 5 minutes, then at 10 minutes, and finally at 20 minutes. If the join is not successful after 20 minutes, then the ASA disables clustering. After you resolve the problem with the data interface, you have to manually enable clustering at the console port by entering `cluster name`, and then `enable`.

- Failed unit—If the unit was removed from the cluster because of a unit health check failure, then rejoining the cluster depends on the source of the failure. For example, a temporary power failure means the unit will rejoin the cluster when it starts up again as long as the cluster control link is up and clustering is still enabled with the `enable` command.

Related Topics
- Configure the Master Unit Bootstrap Settings, page 8-47

Data Path Connection State Replication

Every connection has one owner and at least one backup owner in the cluster. The backup owner does not take over the connection in the event of a failure; instead, it stores TCP/UDP state information, so that the connection can be seamlessly transferred to a new owner in case of a failure.

If the owner becomes unavailable, the first unit to receive packets from the connection (based on load balancing) contacts the backup owner for the relevant state information so it can become the new owner.

Some traffic requires state information above the TCP or UDP layer. See the following table for clustering support or lack of support for this kind of traffic.

Table 8-1  ASA Features Replicated Across the Cluster

<table>
<thead>
<tr>
<th>Traffic</th>
<th>State Support</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up time</td>
<td>Yes</td>
<td>Keeps track of the system up time.</td>
</tr>
<tr>
<td>ARP Table</td>
<td>Yes</td>
<td>Transparent mode only.</td>
</tr>
<tr>
<td>MAC address table</td>
<td>Yes</td>
<td>Transparent mode only.</td>
</tr>
<tr>
<td>User Identity</td>
<td>Yes</td>
<td>Includes AAA rules (uauth) and identify firewall.</td>
</tr>
<tr>
<td>IPv6 Neighbor database</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Dynamic routing</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>SNMP Engine ID</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>VPN (Site-to-Site)</td>
<td>No</td>
<td>VPN sessions will be disconnected if the master unit fails.</td>
</tr>
</tbody>
</table>
**Configuration Replication**

All units in the cluster share a single configuration. Except for the initial bootstrap configuration, you can only make configuration changes on the master unit, and changes are automatically replicated to all other units in the cluster.

**ASA Cluster Management**

One of the benefits of using ASA clustering is the ease of management. This section describes how to manage the cluster.

- Management Network, page 8-11
- Management Interface, page 8-11
- Master Unit Management Vs. Slave Unit Management, page 8-12
- RSA Key Replication, page 8-12
- ASDM Connection Certificate IP Address Mismatch, page 8-12

**Management Network**

We recommend connecting all units to a single management network. This network is separate from the cluster control link.

**Management Interface**

For the management interface, we recommend using one of the dedicated management interfaces. You can configure the management interfaces as Individual interfaces (for both routed and transparent modes) or as a Spanned EtherChannel interface.

We recommend using Individual interfaces for management, even if you use Spanned EtherChannels for your data interfaces. Individual interfaces let you connect directly to each unit if necessary, while a Spanned EtherChannel interface only allows remote connection to the current master unit.

If you use Spanned EtherChannel interface mode, and configure the management interface as an Individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.

For an Individual interface, the Main cluster IP address is a fixed address for the cluster that always belongs to the current master unit. For each interface, you also configure a range of addresses so that each unit, including the current master, can use a Local address from the range. The Main cluster IP address provides consistent management access to an address; when a master unit changes, the Main cluster IP address moves to the new master unit, so management of the cluster continues seamlessly. The Local IP address is used for routing, and is also useful for troubleshooting.

For example, you can manage the cluster by connecting to the Main cluster IP address, which is always attached to the current master unit. To manage an individual member, you can connect to the Local IP address.

For outbound management traffic such as TFTP or syslog, each unit, including the master unit, uses the Local IP address to connect to the server.
For a Spanned EtherChannel interface, you can only configure one IP address, and that IP address is always attached to the master unit. You cannot connect directly to a slave unit using the EtherChannel interface; we recommend configuring the management interface as an Individual interface so that you can connect to each unit. Note that you can use a device-local EtherChannel for management.

**Master Unit Management Vs. Slave Unit Management**

Aside from the bootstrap configuration, all management and monitoring can take place on the master unit. From the master unit, you can check runtime statistics, resource usage, or other monitoring information of all units. You can also issue a command to all units in the cluster, and replicate the console messages from slave units to the master unit.

You can monitor slave units directly if desired. Although also available from the master unit, you can perform file management on slave units (including backing up the configuration and updating images). The following functions are not available from the master unit:

- Monitoring per-unit cluster-specific statistics.
- Syslog monitoring per unit.
- SNMP
- NetFlow

**RSA Key Replication**

When you create an RSA key on the master unit, the key is replicated to all slave units. If you have an SSH session to the Main cluster IP address, you will be disconnected if the master unit fails. The new master unit uses the same key for SSH connections, so that you do not need to update the cached SSH host key when you reconnect to the new master unit.

**ASDM Connection Certificate IP Address Mismatch**

By default, a self-signed certificate is used for the ASDM connection based on the Local IP address. If you connect to the Main cluster IP address using ASDM, then a warning message about a mismatched IP address appears because the certificate uses the Local IP address, and not the Main cluster IP address. You can ignore the message and establish the ASDM connection. However, to avoid this type of warning, you can enroll a certificate that contains the Main cluster IP address and all the Local IP addresses from the IP address pool. You can then use this certificate for each cluster member.

**Related Topics**

- Chapter 34, “Digital Certificates.”

**Load Balancing Methods**

Available load balancing methods depend on the firewall mode and interface type.

- Spanned EtherChannel (Recommended), page 8-13
- Policy-Based Routing (Routed Firewall Mode Only), page 8-17
- Equal-Cost Multi-Path Routing (Routed Firewall Mode Only), page 8-18
Spanned EtherChannel (Recommended)

You can group one or more interfaces per unit into an EtherChannel that spans all units in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel.

- Spanned EtherChannel Benefits, page 8-13
- Guidelines for Maximum Throughput, page 8-13
- Load Balancing, page 8-13
- EtherChannel Redundancy, page 8-14
- Connecting to a VSS or vPC, page 8-14

Spanned EtherChannel Benefits

The EtherChannel method of load-balancing is recommended over other methods for the following benefits:

- Faster failure discovery.
- Faster convergence time. Individual interfaces rely on routing protocols to load-balance traffic, and routing protocols often have slow convergence during a link failure.
- Ease of configuration.

Related Topics
EtherChannels, page 9-5

Guidelines for Maximum Throughput

To achieve maximum throughput, we recommend the following:

- Use a load balancing hash algorithm that is “symmetric,” meaning that packets from both directions will have the same hash, and will be sent to the same ASA in the Spanned EtherChannel. We recommend using the source and destination IP address (the default) or the source and destination port as the hashing algorithm.
- Use the same type of line cards when connecting the ASAs to the switch so that hashing algorithms applied to all packets are the same.

Load Balancing

The EtherChannel link is selected using a proprietary hash algorithm, based on source or destination IP addresses and TCP and UDP port numbers.

Note

On the ASA, do not change the load-balancing algorithm from the default. On the switch, we recommend that you use one of the following algorithms: source-dest-ip or source-dest-ip-port (see the Cisco Nexus OS or Cisco IOS port-channel load-balance command). Do not use a vlan keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the ASAs in a cluster.

The number of links in the EtherChannel affects load balancing.

Symmetric load balancing is not always possible. If you configure NAT, then forward and return packets will have different IP addresses and/or ports. Return traffic will be sent to a different unit based on the hash, and the cluster will have to redirect most returning traffic to the correct unit.
Related Topics

- Customize the EtherChannel, page 9-20
- Load Balancing, page 9-7
- NAT and Clustering, page 8-29

EtherChannel Redundancy

The EtherChannel has built-in redundancy. It monitors the line protocol status of all links. If one link fails, traffic is re-balanced between remaining links. If all links in the EtherChannel fail on a particular unit, but other units are still active, then the unit is removed from the cluster.

Connecting to a VSS or vPC

You can include multiple interfaces per ASA in the Spanned EtherChannel. Multiple interfaces per ASA are especially useful for connecting to both switches in a VSS or vPC.

Depending on your switches, you can configure up to 32 active links in the spanned EtherChannel. This feature requires both switches in the vPC to support EtherChannels with 16 active links each (for example the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module).

For switches that support 8 active links in the EtherChannel, you can configure up to 16 active links in the spanned EtherChannel when connecting to two switches in a VSS/vPC.

If you want to use more than 8 active links in a spanned EtherChannel, you cannot also have standby links; the support for 9 to 32 active links requires you to disable cLACP dynamic port priority that allows the use of standby links. You can still use 8 active links and 8 standby links if desired, for example, when connecting to a single switch.
The following figure shows a 32 active link spanned EtherChannel in an 8-ASA cluster and a 16-ASA cluster.
The following figure shows a 16 active link spanned EtherChannel in a 4-ASA cluster and an 8-ASA cluster.

The following figure shows a traditional 8 active/8 standby link spanned EtherChannel in a 4-ASA cluster and an 8-ASA cluster. The active links are shown as solid lines, while the inactive links are dotted. cLACP load-balancing can automatically choose the best 8 links to be active in the EtherChannel. As shown, cLACP helps achieve load balancing at the link level.
Policy-Based Routing (Routed Firewall Mode Only)

When using Individual interfaces, each ASA interface maintains its own IP address and MAC address. One method of load balancing is Policy-Based Routing (PBR).

We recommend this method if you are already using PBR, and want to take advantage of your existing infrastructure. This method might offer additional tuning options vs. Spanned EtherChannel as well.

PBR makes routing decisions based on a route map and ACL. You must manually divide traffic between all ASAs in a cluster. Because PBR is static, it may not achieve the optimum load balancing result at all times. To achieve the best performance, we recommend that you configure the PBR policy so that forward and return packets of a connection are directed to the same physical ASA. For example, if you have a Cisco router, redundancy can be achieved by using Cisco IOS PBR with Object Tracking. Cisco IOS Object Tracking monitors each ASA using ICMP ping. PBR can then enable or disable route maps based on reachability of a particular ASA. See the following URL for more details:


Note

If you use this method of load-balancing, you can use a device-local EtherChannel as an Individual interface.
Equal-Cost Multi-Path Routing (Routed Firewall Mode Only)

When using Individual interfaces, each ASA interface maintains its own IP address and MAC address. One method of load balancing is Equal-Cost Multi-Path (ECMP) routing.

We recommend this method if you are already using ECMP, and want to take advantage of your existing infrastructure. This method might offer additional tuning options vs. Spanned EtherChannel as well.

ECMP routing can forward packets over multiple “best paths” that tie for top place in the routing metric. Like EtherChannel, a hash of source and destination IP addresses and/or source and destination ports can be used to send a packet to one of the next hops. If you use static routes for ECMP routing, then an ASA failure can cause problems; the route continues to be used, and traffic to the failed ASA will be lost. If you use static routes, be sure to use a static route monitoring feature such as Object Tracking. We recommend using dynamic routing protocols to add and remove routes, in which case, you must configure each ASA to participate in dynamic routing.

Note

If you use this method of load-balancing, you can use a device-local EtherChannel as an Individual interface.

Inter-Site Clustering

For inter-site installations, you can take advantage of ASA clustering as long as you follow these guidelines:

- Inter-Site Clustering Guidelines, page 8-18
- Sizing the Data Center Interconnect, page 8-19
- Inter-Site Examples, page 8-20

Inter-Site Clustering Guidelines

See the following guidelines for inter-site clustering:

- Supports inter-site clustering in the following interface and firewall modes:

<table>
<thead>
<tr>
<th>Interface Mode</th>
<th>Firewall Mode</th>
<th>Fireway Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td>Individual Interface</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Spanned EtherChannel</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- The cluster control link latency must be less than 20 ms round-trip time (RTT).
- The cluster control link must be reliable, with no out-of-order or dropped packets; for example, you should use a dedicated link.
- Do not configure connection rebalancing; you do not want connections rebalanced to cluster members at a different site.
- The cluster implementation does not differentiate between members at multiple sites; therefore, connection roles for a given connection may span across sites. This is expected behavior.
For transparent mode, if the cluster is placed between a pair of inside and outside routers (AKA North-South insertion), you must ensure that both inside routers share a MAC address, and also that both outside routers share a MAC address. When a cluster member at site 1 forwards a connection to a member at site 2, the destination MAC address is preserved. The packet will only reach the router at site 2 if the MAC address is the same as the router at site 1.

For transparent mode, if the cluster is placed between data networks and the gateway router at each site for firewalling between internal networks (AKA East-West insertion), then each gateway router should use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide identical virtual IP and MAC address destinations at each site. The data VLANs are extended across the sites using Overlay Transport Virtualization (OTV), or something similar. You need to create filters to prevent traffic that is destined to the local gateway router from being sent over the DCI to the other site. If the gateway router becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site’s gateway.

Related Topics
- Rebalancing New TCP Connections Across the Cluster, page 8-24
- Connection Roles, page 8-23

Sizing the Data Center Interconnect

You should reserve bandwidth on the data center interconnect (DCI) for cluster control link traffic equivalent to the following calculation:

\[
\text{Reserved DCI bandwidth} = \left( \frac{\text{# of cluster members per site}}{2} \right) \times \text{cluster control link size per member}
\]

If the number of members differs at each site, use the larger number for your calculation. The minimum bandwidth for the DCI should not be less than the size of the cluster control link for one member.

For example:

- For 4 members at 2 sites:
  - 4 cluster members total
  - 2 members at each site
  - 5 Gbps cluster control link per member
  
  Reserved DCI bandwidth = 5 Gbps (2/2 x 5 Gbps).

- For 8 members at 2 sites, the size increases:
  - 8 cluster members total
  - 4 members at each site
  - 5 Gbps cluster control link per member
  
  Reserved DCI bandwidth = 10 Gbps (4/2 x 5 Gbps).

- For 6 members at 3 sites:
  - 6 cluster members total
  - 3 members at site 1, 2 members at site 2, and 1 member at site 3
  - 10 Gbps cluster control link per member
  
  Reserved DCI bandwidth = 15 Gbps (3/2 x 10 Gbps).
• For 2 members at 2 sites:
  – 2 cluster members total
  – 1 member at each site
  – 10 Gbps cluster control link per member

Reserved DCI bandwidth = 10 Gbps (1/2 x 10 Gbps = 5 Gbps; but the minimum bandwidth should not be less than the size of the cluster control link (10 Gbps)).

Inter-Site Examples

The following examples show supported cluster deployments.

• Individual Interface Routed Mode North-South Inter-Site Example, page 8-20
• Spanned EtherChannel Transparent Mode North-South Inter-Site Example, page 8-21
• Spanned EtherChannel Transparent Mode East-West Inter-Site Example, page 8-22

Individual Interface Routed Mode North-South Inter-Site Example

The following example shows 2 ASA cluster members at each of 2 data centers placed between inside and outside routers (North-South insertion). The cluster members are connected by the cluster control link over the DCI. The inside and outside routers at each data center use OSPF and PBR or ECMP to load balance the traffic between cluster members. By assigning a higher cost route across the DCI, traffic stays within each data center unless all ASA cluster members at a given site go down. In the event of a failure of all cluster members at one site, traffic goes from each router over the DCI to the ASA cluster members at the other site.
Spanned EtherChannel Transparent Mode North-South Inter-Site Example

The following example shows 2 ASA cluster members at each of 2 data centers placed between inside and outside routers (North-South insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for the inside and outside. Each ASA EtherChannel is spanned across all ASAs in the cluster.

The inside and outside routers at each data center use OSPF, which is passed through the transparent ASAs. Unlike MACs, router IPs are unique on all routers. By assigning a higher cost route across the DCI, traffic stays within each data center unless all ASA cluster members at a given site go down. The lower cost route through the ASAs must traverse the same bridge group at each site for the cluster to maintain asymmetric connections. In the event of a failure of all cluster members at one site, traffic goes from each router over the DCI to the ASA cluster members at the other site.

The implementation of the switches at each site can include:

- **Inter-site VSS/vPC**—In this scenario, you install one switch at Data Center 1, and the other at Data Center 2. One option is for the ASA cluster units at each Data Center to only connect to the local switch, while the VSS/vPC traffic goes across the DCI. In this case, connections are for the most part kept local to each datacenter. You can optionally connect each ASA unit to both switches across the DCI if the DCI can handle the extra traffic. In this case, traffic is distributed across the data centers, so it is essential for the DCI to be very robust.

- **Local VSS/vPC at each site**—For better switch redundancy, you can install 2 separate VSS/vPC pairs at each site. In this case, although the ASAs still have a spanned EtherChannel with Data Center 1 ASAs connected only to both local switches, and Data Center 2 ASAs connected to those local switches, the spanned EtherChannel is essentially “split.” Each local VSS/vPC sees the spanned EtherChannel as a site-local EtherChannel.
Spanned EtherChannel Transparent Mode East-West Inter-Site Example

The following example shows 2 ASA cluster members at each of 2 data centers placed between the gateway router and two inside networks at each site, the App network and the DB network (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the App and DB networks on the inside and outside. Each ASA EtherChannel is spanned across all ASAs in the cluster.

The gateway router at each site uses an FHRP such as HSRP to provide the same destination virtual MAC and IP addresses at each site. The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters to prevent traffic from traversing the DCI to the other site when the traffic is destined for the gateway router. If the gateway router at one site becomes unreachable, you must remove the filters so traffic can be sent to the other site’s gateway router.

See Spanned EtherChannel Transparent Mode North-South Inter-Site Example, page 8-21 for information about vPC/VSS options.

How the ASA Cluster Manages Connections

Connections can be load-balanced to multiple members of the cluster. Connection roles determine how to connections are handled in both normal operation and in a high availability situation.

- Connection Roles, page 8-23
- New Connection Ownership, page 8-23
Connection Roles

There are 3 different ASA roles defined for each connection:

- **Owner**—The unit that initially receives the connection. The owner maintains the TCP state and processes packets. A connection has only one owner.
- **Director**—The unit that handles owner lookup requests from forwarders and also maintains the connection state to serve as a backup if the owner fails. When the owner receives a new connection, it chooses a director based on a hash of the source/destination IP address and TCP ports, and sends a message to the director to register the new connection. If packets arrive at any unit other than the owner, the unit queries the director about which unit is the owner so it can forward the packets. A connection has only one director.
- **Forwarder**—A unit that forwards packets to the owner. If a forwarder receives a packet for a connection it does not own, it queries the director for the owner, and then establishes a flow to the owner for any other packets it receives for this connection. The director can also be a forwarder. Note that if a forwarder receives the SYN-ACK packet, it can derive the owner directly from a SYN cookie in the packet, so it does not need to query the director. (If you disable TCP sequence randomization, the SYN cookie is not used; a query to the director is required.) For short-lived flows such as DNS and ICMP, instead of querying, the forwarder immediately sends the packet to the director, which then sends them to the owner. A connection can have multiple forwarders; the most efficient throughput is achieved by a good load-balancing method where there are no forwarders and all packets of a connection are received by the owner.

New Connection Ownership

When a new connection is directed to a member of the cluster via load balancing, that unit owns both directions of the connection. If any connection packets arrive at a different unit, they are forwarded to the owner unit over the cluster control link. For best performance, proper external load balancing is required for both directions of a flow to arrive at the same unit, and for flows to be distributed evenly between units. If a reverse flow arrives at a different unit, it is redirected back to the original unit.

Related Topics

- Load Balancing Methods, page 8-12

Sample Data Flow

The following example shows the establishment of a new connection.
1. The SYN packet originates from the client and is delivered to an ASA (based on the load balancing method), which becomes the owner. The owner creates a flow, encodes owner information into a SYN cookie, and forwards the packet to the server.

2. The SYN-ACK packet originates from the server and is delivered to a different ASA (based on the load balancing method). This ASA is the forwarder.

3. Because the forwarder does not own the connection, it decodes owner information from the SYN cookie, creates a forwarding flow to the owner, and forwards the SYN-ACK to the owner.

4. The owner sends a state update to the director, and forwards the SYN-ACK to the client.

5. The director receives the state update from the owner, creates a flow to the owner, and records the TCP state information as well as the owner. The director acts as the backup owner for the connection.

6. Any subsequent packets delivered to the forwarder will be forwarded to the owner.

7. If packets are delivered to any additional units, it will query the director for the owner and establish a flow.

8. Any state change for the flow results in a state update from the owner to the director.

**Rebalancing New TCP Connections Across the Cluster**

If the load balancing capabilities of the upstream or downstream routers result in unbalanced flow distribution, you can configure overloaded units to redirect new TCP flows to other units. No existing flows will be moved to other units.

**ASA Features and Clustering**

Some ASA features are not supported with ASA clustering, and some are only supported on the master unit. Other features might have caveats for proper usage.

- Unsupported Features with Clustering, page 8-25
- Centralized Features for Clustering, page 8-26
• Features Applied to Individual Units, page 8-26
• Dynamic Routing and Clustering, page 8-27
• Multicast Routing and Clustering, page 8-29
• NAT and Clustering, page 8-29
• AAA for Network Access and Clustering, page 8-30
• Syslog and NetFlow and Clustering, page 8-31
• SNMP and Clustering, page 8-31
• VPN and Clustering, page 8-31
• FTP and Clustering, page 8-31
• Cisco TrustSec and Clustering, page 8-32

Unsupported Features with Clustering

These features cannot be configured with clustering enabled, and the commands will be rejected.

• Unified Communications
• Remote access VPN (SSL VPN and IPsec VPN)
• The following application inspections:
  – CTIQBE
  – GTP
  – H323, H225, and RAS
  – IPsec passthrough
  – MGCP
  – MMP
  – RTSP
  – SIP
  – SCCP (Skinny)
  – WAAS
  – WCCP
• Botnet Traffic Filter
• Auto Update Server
• DHCP client, server, relay, and proxy
• VPN load balancing
• Failover
• ASA CX module
Centralized Features for Clustering

The following features are only supported on the master unit, and are not scaled for the cluster. For example, you have a cluster of eight units (5585-X with SSP-60). The Other VPN license allows a maximum of 10,000 site-to-site IPSec tunnels for one ASA 5585-X with SSP-60. For the entire cluster of eight units, you can only use 10,000 tunnels; the feature does not scale.

Note
Traffic for centralized features is forwarded from member units to the master unit over the cluster control link.

If you use the rebalancing feature, traffic for centralized features may be rebalanced to non-master units before the traffic is classified as a centralized feature; if this occurs, the traffic is then sent back to the master unit.

For centralized features, if the master unit fails, all connections are dropped, and you have to re-establish the connections on the new master unit.

- Site-to-site VPN
- The following application inspections:
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- Dynamic routing (Spanned EtherChannel mode only)
- Multicast routing (Individual interface mode only)
- Static route monitoring
- IGMP multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- PIM multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- Authentication and Authorization for network access. Accounting is decentralized.
- Filtering Services

Related Topics
- Size the Cluster Control Link, page 8-7
- Rebalancing New TCP Connections Across the Cluster, page 8-24

Features Applied to Individual Units

These features are applied to each ASA unit, instead of the cluster as a whole or to the master unit.
• QoS—The QoS policy is synced across the cluster as part of configuration replication. However, the policy is enforced on each unit independently. For example, if you configure policing on output, then the conform rate and conform burst values are enforced on traffic exiting a particular ASA. In a cluster with 8 units and with traffic evenly distributed, the conform rate actually becomes 8 times the rate for the cluster.

• Threat detection—Threat detection works on each unit independently; for example, the top statistics is unit-specific. Port scanning detection, for example, does not work because scanning traffic will be load-balanced between all units, and one unit will not see all traffic.

• Resource management—Resource management in multiple context mode is enforced separately on each unit based on local usage.

• ASA FirePOWER module—There is no configuration sync or state sharing between ASA FirePOWER modules. You are responsible for maintaining consistent policies on the ASA FirePOWER modules in the cluster using FireSIGHT Management Center. Do not use different ASA-interface-based zone definitions for devices in the cluster.

• ASA IPS module—There is no configuration sync or state sharing between IPS modules. Some IPS signatures require IPS to keep the state across multiple connections. For example, the port scanning signature is used when the IPS module detects that someone is opening many connections to one server but with different ports. In clustering, those connections will be balanced between multiple ASA devices, each of which has its own IPS module. Because these IPS modules do not share state information, the cluster may not be able to detect port scanning as a result.

Dynamic Routing and Clustering

• **Dynamic Routing in Spanned EtherChannel Mode, page 8-27**

• **Dynamic Routing in Individual Interface Mode, page 8-28**

**Dynamic Routing in Spanned EtherChannel Mode**

In Spanned EtherChannel mode, the routing process only runs on the master unit, and routes are learned through the master unit and replicated to slaves. If a routing packet arrives at a slave, it is redirected to the master unit.
About ASA Clustering

After the slave members learn the routes from the master unit, each unit makes forwarding decisions independently.

The OSPF LSA database is not synchronized from the master unit to slave units. If there is a master unit switchover, the neighboring router will detect a restart; the switchover is not transparent. The OSPF process picks an IP address as its router ID. Although not required, you can assign a static router ID to ensure a consistent router ID is used across the cluster. See the OSPF Non-Stop Forwarding feature to address the interruption.

Dynamic Routing in Individual Interface Mode

In Individual interface mode, each unit runs the routing protocol as a standalone router, and routes are learned by each unit independently.
In the above diagram, Router A learns that there are 4 equal-cost paths to Router B, each through an ASA. ECMP is used to load balance traffic between the 4 paths. Each ASA picks a different router ID when talking to external routers.

You must configure a cluster pool for the router ID so that each unit has a separate router ID.

**Multicast Routing and Clustering**

Multicast routing behaves differently depending on the interface mode.

- Multicast Routing in Spanned EtherChannel Mode, page 8-29
- Multicast Routing in Individual Interface Mode, page 8-29

**Multicast Routing in Spanned EtherChannel Mode**

In Spanned EtherChannel mode, the master unit handles all multicast routing packets and data packets until fast-path forwarding is established. After the connection is established, each slave can forward multicast data packets.

**Multicast Routing in Individual Interface Mode**

In Individual interface mode, units do not act independently with multicast. All data and routing packets are processed and forwarded by the master unit, thus avoiding packet replication.

**NAT and Clustering**

NAT can impact the overall throughput of the cluster. Inbound and outbound NAT packets can be sent to different ASAs in the cluster because the load balancing algorithm relies on IP addresses and ports, and NAT causes inbound and outbound packets to have different IP addresses and/or ports. When a packet arrives at an ASA that is not the connection owner, it is forwarded over the cluster control link to the owner, causing large amounts of traffic on the cluster control link.
If you still want to use NAT in clustering, then consider the following guidelines:

- No Proxy ARP—For Individual interfaces, a proxy ARP reply is never sent for mapped addresses. This prevents the adjacent router from maintaining a peer relationship with an ASA that may no longer be in the cluster. The upstream router needs a static route or PBR with Object Tracking for the mapped addresses that points to the Main cluster IP address. This is not an issue for a Spanned EtherChannel, because there is only one IP address associated with the cluster interface.

- No interface PAT on an Individual interface—Interface PAT is not supported for Individual interfaces.

- NAT pool address distribution for dynamic PAT—The master unit evenly pre-distributes addresses across the cluster. If a member receives a connection and they have no addresses left, the connection is dropped, even if other members still have addresses available. Make sure to include at least as many NAT addresses as there are units in the cluster to ensure that each unit receives an address. Use the `show nat pool cluster` command to see the address allocations.

- No round-robin—Round-robin for a PAT pool is not supported with clustering.

- Dynamic NAT translates managed by the master unit—The master unit maintains and replicates the translate table to slave units. When a slave unit receives a connection that requires dynamic NAT, and the translate is not in the table, it requests the translate from the master unit. The slave unit owns the connection.

- Per-session PAT feature—Although not exclusive to clustering, the per-session PAT feature improves the scalability of PAT and, for clustering, allows each slave unit to own PAT connections; by contrast, multi-session PAT connections have to be forwarded to and owned by the master unit. By default, all TCP traffic and UDP DNS traffic use a per-session PAT translate. For traffic that requires multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT. For more information about per-session PAT, see the firewall configuration guide.

- No static PAT for the following inspections—
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - All Voice-over-IP applications

### AAA for Network Access and Clustering

AAA for network access consists of three components: authentication, authorization, and accounting. Authentication and accounting are implemented as centralized features on the clustering master with replication of the data structures to the cluster slaves. If a master is elected, the new master will have all the information it needs to continue uninterrupted operation of the established authenticated users and their associated authorizations. Idle and absolute timeouts for user authentications are preserved when a master unit change occurs.

Accounting is implemented as a distributed feature in a cluster. Accounting is done on a per-flow basis, so the cluster unit owning a flow will send accounting start and stop messages to the AAA server when accounting is configured for a flow.
Syslog and NetFlow and Clustering

- Syslog—Each unit in the cluster generates its own syslog messages. You can configure logging so that each unit uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all units in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all units look as if they come from a single unit. If you configure logging to use the local-unit name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different units.

- NetFlow—Each unit in the cluster generates its own NetFlow stream. The NetFlow collector can only treat each ASA as a separate NetFlow exporter.

Related Topics
- Include the Device ID in Non-EMBLEM Format Syslog Messages, page 39-16

SNMP and Clustering

An SNMP agent polls each individual ASA by its Local IP address. You cannot poll consolidated data for the cluster.

You should always use the Local address, and not the Main cluster IP address for SNMP polling. If the SNMP agent polls the Main cluster IP address, if a new master is elected, the poll to the new master unit will fail.

VPN and Clustering

Site-to-site VPN is a centralized feature; only the master unit supports VPN connections.

Note
Remote access VPN is not supported with clustering.

VPN functionality is limited to the master unit and does not take advantage of the cluster high availability capabilities. If the master unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new master is elected, you must reestablish the VPN connections.

When you connect a VPN tunnel to a Spanned EtherChannel address, connections are automatically forwarded to the master unit. For connections to an Individual interface when using PBR or ECMP, you must always connect to the Main cluster IP address, not a Local address.

VPN-related keys and certificates are replicated to all units.

FTP and Clustering

- If FTP data channel and control channel flows are owned by different cluster members, the data channel owner will periodically send idle timeout updates to the control channel owner and update the idle timeout value. However, if the control flow owner is reloaded, and the control flow is re-hosted, the parent/child flow relationship will not longer be maintained; the control flow idle timeout will not be updated.

- If you use AAA for FTP access, then the control channel flow is centralized on the master unit.
Cisco TrustSec and Clustering

Only the master unit learns security group tag (SGT) information. The master unit then populates the SGT to slaves, and slaves can make a match decision for SGT based on the security policy.

Licensing for ASA Clustering

Cluster units do not require the same license on each unit. Typically, you buy a license only for the master unit; slave units inherit the master license. If you have licenses on multiple units, they combine into a single running ASA cluster license.

There are exceptions to this rule. See the following table for precise licensing requirements for clustering.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5585-X</td>
<td>Cluster License, supports up to 16 units. Note: Each unit must have the same encryption license; each unit must have the same 10 GE I/O/Security Plus license (ASA 5585-X with SSP-10 and -20).</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>Security Plus license, supports 2 units. Note: Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X</td>
<td>Base License, supports 2 units. Note: Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>All other models</td>
<td>No support.</td>
</tr>
</tbody>
</table>

Prerequisites for ASA Clustering

ASA Hardware and Software Requirements

All units in a cluster:
- Must be the same model with the same DRAM. You do not have to have the same amount of flash memory.
- Must run the identical software except at the time of an image upgrade. Hitless upgrade is supported.
- You can have cluster members in different geographical locations (inter-site) when using individual interface mode.
- Must be in the same security context mode, single or multiple.
- (Single context mode) Must be in the same firewall mode, routed or transparent.
- New cluster members must use the same SSL encryption setting (the ssl encryption command) as the master unit for initial cluster control link communication before configuration replication.
- Must have the same cluster, encryption and, for the ASA 5585-X, 10 GE I/O licenses.

Switch Prerequisites

- Be sure to complete the switch configuration before you configure clustering on the ASAs.
Guidelines for ASA Clustering

Context Mode
The mode must match on each member unit.

Firewall Mode
For single mode, the firewall mode must match on all units.

Failover
Failover is not supported with clustering.

IPv6
The cluster control link is only supported using IPv4.

Models
Supported on:
- ASA 5585-X

For the ASA 5585-X with SSP-10 and SSP-20, which include two Ten Gigabit Ethernet interfaces, we recommend using one interface for the cluster control link, and the other for data (you can use subinterfaces for data). Although this setup does not accommodate redundancy for the cluster control link, it does satisfy the need to size the cluster control link to match the size of the data interfaces.

- For a list of supported switches, see Cisco ASA Compatibility.

ASA Prerequisites
- Provide each unit with a unique IP address before you join them to the management network.
  - See the Getting Started chapter for more information about connecting to the ASA and setting the management IP address.
  - Except for the IP address used by the master unit (typically the first unit you add to the cluster), these management IP addresses are for temporary use only.
  - After a slave joins the cluster, its management interface configuration is replaced by the one replicated from the master unit.
- To use jumbo frames on the cluster control link (recommended), you must enable Jumbo Frame Reservation before you enable clustering.

Other Prerequisites
We recommend using a terminal server to access all cluster member unit console ports. For initial setup, and ongoing management (for example, when a unit goes down), a terminal server is useful for remote management.

Related Topics
- Guidelines for ASA Clustering, page 8-33
- Enable Jumbo Frame Support, page 9-22
- Bootstrap Configuration, page 8-3
**Switches**

- On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the ASA to speed up the join process for new units.
- When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an Individual interface on the switch.
- On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: `source-dest-ip` or `source-dest-ip-port` (see the Cisco Nexus OS and Cisco IOS `port-channel load-balance` command). Do not use a `vlan` keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the ASAs in a cluster. Do not change the load-balancing algorithm from the default on the ASA (in the `port-channel load-balance` command).
- If you change the load-balancing algorithm of the EtherChannel on the switch, the EtherChannel interface on the switch temporarily stops forwarding traffic, and the Spanning Tree Protocol restarts. There will be a delay before traffic starts flowing again.
- You should disable the LACP Graceful Convergence feature on all cluster-facing EtherChannel interfaces for Cisco Nexus switches.
- Some switches do not support dynamic port priority with LACP (active and standby links). You can disable dynamic port priority to provide better compatibility with spanned EtherChannels.
- Network elements on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.
- Port-channel bundling downtime should not exceed the configured keepalive interval.
- On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the ASA to fixed:

  ```
  router(config)# port-channel id hash-distribution fixed
  ```

  Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.

**EtherChannels**

- The ASA does not support connecting an EtherChannel to a switch stack. If the ASA EtherChannel is connected cross stack, and if the master switch is powered down, then the EtherChannel connected to the remaining switch will not come up.
- Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.
  - Spanned EtherChannels—For ASA Spanned EtherChannels, which span across all members of the cluster, the interfaces are combined into a single EtherChannel on the switch. Make sure each interface is in the same channel group on the switch.
Device-local EtherChannels—For ASA Device-local EtherChannels including any EtherChannels configured for the cluster control link, be sure to configure discrete EtherChannels on the switch; do not combine multiple ASA EtherChannels into one EtherChannel on the switch.
Additional Guidelines

- When significant topology changes occur (such as adding or removing an EtherChannel interface, enabling or disabling an interface on the ASA or the switch, adding an additional switch to form a VSS or vPC) you should disable the health check feature. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the health check feature.

- When adding a unit to an existing cluster, or when reloading a unit, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang your connection; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.

- If you use a Windows 2003 server connected to a Spanned EtherChannel, when the syslog server port is down and the server does not throttle ICMP error messages, then large numbers of ICMP messages are sent back to the ASA cluster. These messages can result in some units of the ASA cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.

Related Topics

- Size the Cluster Control Link, page 8-7
- Bootstrap Configuration, page 8-3
- Unsupported Features with Clustering, page 8-25
- Configure an EtherChannel, page 9-18
• EtherChannels, page 9-12

Defaults for ASA Clustering

• When using Spanned EtherChannels, the cLACP system ID is auto-generated and the system priority is 1 by default.
• The cluster health check feature is enabled by default with the holdtime of 3 seconds.
• Connection rebalancing is disabled by default. If you enable connection rebalancing, the default time between load information exchanges is 5 seconds.

Configure ASA Clustering

Note To enable or disable clustering, you must use a console connection (for CLI) or an ASDM connection.

To configure clustering, perform the following tasks:

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Complete all pre-configuration on the switches and ASAs according to Prerequisites for ASA Clustering, page 8-32 and Guidelines for ASA Clustering, page 8-33.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Cable the Cluster Units and Configure Upstream and Downstream Equipment, page 8-37.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the Cluster Interface Mode on Each Unit, page 8-39. You can only configure one type of interface for clustering: Spanned EtherChannels or Individual interfaces.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure Interfaces on the Master Unit, page 8-40. You cannot enable clustering if the interfaces are not cluster-ready.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure the Master Unit Bootstrap Settings, page 8-47.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure Slave Unit Bootstrap Settings, page 8-52.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Configure the security policy on the master unit. See the chapters in this guide to configure supported features on the master unit. The configuration is replicated to the slave units.</td>
</tr>
</tbody>
</table>

Cable the Cluster Units and Configure Upstream and Downstream Equipment

Before configuring clustering, cable the cluster control link network, management network, and data networks.

Note At a minimum, an active cluster control link network is required before you configure the units to join the cluster.

You should also configure the upstream and downstream equipment. For example, if you use EtherChannels, then you should configure the upstream and downstream equipment for the EtherChannels.
Examples

Note

This example uses EtherChannels for load-balancing. If you are using PBR or ECMP, your switch configuration will differ.

For example on each of 4 ASA 5585-Xs, you want to use:

- 2 Ten Gigabit Ethernet interfaces in a device-local EtherChannel for the cluster control link.
- 2 Ten Gigabit Ethernet interfaces in a Spanned EtherChannel for the inside and outside network; each interface is a VLAN subinterface of the EtherChannel. Using subinterfaces lets both inside and outside interfaces take advantage of the benefits of an EtherChannel.
- 1 Management interface.

You have one switch for both the inside and outside networks.
Configure ASA Clustering

Configure ASA Clustering

Table: Connect Interfaces on each of 4 ASAs

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Connect Interfaces on each of 4 ASAs</th>
<th>To Switch Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster control link</td>
<td>TenGigabitEthernet 0/6 and TenGigabitEthernet 0/7</td>
<td>8 ports total</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For each TenGigabitEthernet 0/6 and TenGigabitEthernet 0/7 pair, configure 4 EtherChannels (1 EC for each ASA). These EtherChannels must all be on the same isolated cluster control VLAN, for example VLAN 101.</td>
</tr>
<tr>
<td>Inside and outside interfaces</td>
<td>TenGigabitEthernet 0/8 and TenGigabitEthernet 0/9</td>
<td>8 ports total</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure a single EtherChannel (across all ASAs). On the switch, configure these VLANs and networks now; for example, a trunk including VLAN 200 for the inside and VLAN 201 for the outside.</td>
</tr>
<tr>
<td>Management interface</td>
<td>Management 0/0</td>
<td>4 ports total</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Place all interfaces on the same isolated management VLAN, for example VLAN 100.</td>
</tr>
</tbody>
</table>

Configure the Cluster Interface Mode on Each Unit

You can only configure one type of interface for clustering: Spanned EtherChannels or Individual interfaces; you cannot mix interface types in a cluster.

Before You Begin

- You must set the mode separately on each ASA that you want to add to the cluster.
- You can always configure the management-only interface as an Individual interface (recommended), even in Spanned EtherChannel mode. The management interface can be an Individual interface even in transparent firewall mode.
- In Spanned EtherChannel mode, if you configure the management interface as an Individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.
- In multiple context mode, you must choose one interface type for all contexts. For example, if you have a mix of transparent and routed mode contexts, you must use Spanned EtherChannel mode for all contexts because that is the only interface type allowed for transparent mode.

Procedure

Step 1  Show any incompatible configuration so that you can force the interface mode and fix your configuration later; the mode is not changed with this command:

```
cluster interface-mode (individual | spanned) check-details
```
Example:
```
ciscoasa(config)# cluster interface-mode spanned check-details
```

**Step 2**
Set the interface mode for clustering:
```
cluster interface-mode {individual | spanned} force
```

Example:
```
ciscoasa(config)# cluster interface-mode spanned force
```

There is no default setting; you must explicitly choose the mode. If you have not set the mode, you cannot enable clustering.

The **force** option changes the mode without checking your configuration for incompatible settings. You need to manually fix any configuration issues after you change the mode. Because any interface configuration can only be fixed after you set the mode, we recommend using the **force** option so that you can at least start from the existing configuration. You can re-run the **check-details** option after you set the mode for more guidance.

Without the **force** option, if there is any incompatible configuration, you are prompted to clear your configuration and reload, thus requiring you to connect to the console port to reconfigure your management access. If your configuration is compatible (rare), the mode is changed and the configuration is preserved. If you do not want to clear your configuration, you can exit the command by typing **n**.

To remove the interface mode, enter the **no cluster interface-mode** command.

---

**Configure Interfaces on the Master Unit**

You must modify any interface that is currently configured with an IP address to be cluster-ready **before** you enable clustering. For other interfaces, you can configure them before or after you enable clustering; we recommend pre-configuring all of your interfaces so that the complete configuration is synced to new cluster members.

This section describes how to configure interfaces to be compatible with clustering. You can configure data interfaces as either Spanned EtherChannels or as Individual interfaces. Each method uses a different load-balancing mechanism. You cannot configure both types in the same configuration, with the exception of the management interface, which can be an Individual interface even in Spanned EtherChannel mode.

- Configure Individual Interfaces (Recommended for the Management Interface), page 8-40
- Configure Spanned EtherChannels, page 8-43

**Related Topics**

- Cluster Interfaces, page 8-4

**Configure Individual Interfaces (Recommended for the Management Interface)**

Individual interfaces are normal routed interfaces, each with their own IP address taken from a pool of IP addresses. The Main cluster IP address is a fixed address for the cluster that always belongs to the current master unit.
In Spanned EtherChannel mode, we recommend configuring the management interface as an Individual interface. Individual management interfaces let you connect directly to each unit if necessary, while a Spanned EtherChannel interface only allows connection to the current master unit.

**Before You Begin**

- Except for the management-only interface, you must be in Individual interface mode.
- For multiple context mode, perform this procedure in each context. If you are not already in the context configuration mode, enter the `change context name` command.
- Individual interfaces require you to configure load balancing on neighbor devices. External load balancing is not required for the management interface.
- (Optional) Configure the interface as a device-local EtherChannel interface, a redundant interface, and/or configure subinterfaces.
  - For an EtherChannel, this EtherChannel is local to the unit, and is not a Spanned EtherChannel.
  - Management-only interfaces cannot be redundant interfaces.

**Procedure**

**Step 1** Configure a pool of Local IP addresses (IPv4 and/or IPv6), one of which will be assigned to each cluster unit for the interface:

(IPv4)

```
ip local pool poolname first-address-last-address [mask mask]
```

(IPv6)

```
ipv6 local pool poolname ipv6-address/prefix-length number_of_addresses
```

Example:
```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
```  
```
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8::1002/32 8
```  

Include at least as many addresses as there are units in the cluster. If you plan to expand the cluster, include additional addresses. The Main cluster IP address that belongs to the current master unit is not a part of this pool; be sure to reserve an IP address on the same network for the Main cluster IP address.

You cannot determine the exact Local address assigned to each unit in advance; to see the address used on each unit, enter the `show ip[v6] local pool poolname` command. Each cluster member is assigned a member ID when it joins the cluster. The ID determines the Local IP used from the pool.

**Step 2** Enter interface configuration mode:

```
interface interface_id
```

Example:
```
ciscoasa(config)# interface tengigabitethernet 0/8
```  

**Step 3** (Management interface only) Set an interface to management-only mode so that it does not pass through traffic:

```
management-only
```

By default, Management type interfaces are configured as management-only. In transparent mode, this command is always enabled for a Management type interface.

This setting is required if the cluster interface mode is Spanned.
Step 4  Name the interface:

```
nameif name
```

Example:
```
ciscoasa(config-if)# nameif inside
```

The `name` is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value.

Step 5  Set the Main cluster IP address and identifies the cluster pool:

(IPv4)
```
ip address ip_address [mask] cluster-pool poolname
```

(IPv6)
```
ipv6 address ipv6-address/prefix-length cluster-pool poolname
```

Example:
```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8::1002/32 cluster-pool insipv6
```

This IP address must be on the same network as the cluster pool addresses, but not be part of the pool. You can configure an IPv4 and/or an IPv6 address.

DHCP, PPPoE, and IPv6 autoconfiguration are not supported; you must manually configure the IP addresses.

Step 6  Set the security level, where `number` is an integer between 0 (lowest) and 100 (highest):

```
security-level number
```

Example:
```
ciscoasa(config-if)# security-level 100
```

Step 7  Enable the interface:

```
no shutdown
```

Examples

The following example configures the Management 0/0 and Management 0/1 interfaces as a device-local EtherChannel, and then configures the EtherChannel as an Individual interface:

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
    channel-group 1 mode active
    no shutdown

interface management 0/1
    channel-group 1 mode active
    no shutdown

interface port-channel 1
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8:45:1001/64 cluster-pool mgmtipv6
```
security-level 100
management-only

Related Topics
- Management Interface, page 8-11
- Configure the Cluster Interface Mode on Each Unit, page 8-39
- Load Balancing Methods, page 8-12
- Configure an EtherChannel, page 9-18
- Configure a Redundant Interface, page 9-16
- Configure VLAN Subinterfaces and 802.1Q Trunking, page 9-21
- Security Levels, page 11-1

Configure Spanned EtherChannels

A Spanned EtherChannel spans all ASAs in the cluster, and provides load balancing as part of the EtherChannel operation.

Before You Begin
- You must be in Spanned EtherChannel interface mode.
- For multiple context mode, start this procedure in the system execution space. If you are not already in the System configuration mode, enter the `changeto system` command.
- For transparent mode, configure the bridge group.
- Do not specify the maximum and minimum links in the EtherChannel—We recommend that you do not specify the maximum and minimum links in the EtherChannel (The `lacp max-bundle` and `port-channel min-bundle` commands) on either the ASA or the switch. If you need to use them, note the following:
  - The maximum links set on the ASA is the total number of active ports for the whole cluster. Be sure the maximum links value configured on the switch is not larger than the ASA value.
  - The minimum links set on the ASA is the minimum active ports to bring up a port-channel interface per unit. On the switch, the minimum links is the minimum links across the cluster, so this value will not match the ASA value.
- Do not change the load-balancing algorithm from the default (see the `port-channel load-balance` command). On the switch, we recommend that you use one of the following algorithms: `source-dest-ip` or `source-dest-ip-port` (see the Cisco Nexus OS and Cisco IOS `port-channel load-balance` command). Do not use a `vlan` keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the ASAs in a cluster.
- The `lacp port-priority` and `lacp system-priority` commands are not used for a Spanned EtherChannel.
- When using Spanned EtherChannels, the port-channel interface will not come up until clustering is fully enabled. This requirement prevents traffic from being forwarded to a unit that is not an active unit in the cluster.

Procedure

**Step 1** Specify the interface you want to add to the channel group:
interface physical_interface

Example:
ciscoasa(config)# interface gigabitethernet 0/0

The physical_interface ID includes the type, slot, and port number as type slot/port. This first interface in the channel group determines the type and speed for all other interfaces in the group.

**Step 2** Assign this interface to an EtherChannel:

channel-group channel_id mode active [vss-id {1 | 2}]

Example:
ciscoasa(config-if)# channel-group 1 mode active

The channel_id is between 1 and 48. If the port-channel interface for this channel ID does not yet exist in the configuration, one will be added automatically:

interface port-channel channel_id

Only active mode is supported for Spanned EtherChannels.

If you are connecting the ASA to two switches in a VSS or vPC, then configure the vss-id keyword to identify to which switch this interface is connected (1 or 2). You must also use the port-channel span-cluster vss-load-balance command for the port-channel interface in Step 6.

**Step 3** Enable the interface:

no shutdown

**Step 4** (Optional) Add additional interfaces to the EtherChannel by repeating Step 1 through Step 3.

Example:
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown

Multiple interfaces in the EtherChannel per unit are useful for connecting to switches in a VSS or vPC. Keep in mind that by default, a spanned EtherChannel can have only 8 active interfaces out of 16 maximum across all members in the cluster; the remaining 8 interfaces are on standby in case of link failure. To use more than 8 active interfaces (but no standby interfaces), disable dynamic port priority using the clacp static-port-priority command. When you disable dynamic port priority, you can use up to 32 active links across the cluster. For example, for a cluster of 16 ASAs, you can use a maximum of 2 interfaces on each ASA, for a total of 32 interfaces in the spanned EtherChannel.

**Step 5** Specify the port-channel interface:

interface port-channel channel_id

Example:
ciscoasa(config)# interface port-channel 1

This interface was created automatically when you added an interface to the channel group.

**Step 6** Set this EtherChannel as a Spanned EtherChannel:

port-channel span-cluster [vss-load-balance]

Example:
ciscoasa(config-if)# port-channel span-cluster
If you are connecting the ASA to two switches in a VSS or vPC, then you should enable VSS load balancing by using the `vss-load-balance` keyword. This feature ensures that the physical link connections between the ASAs to the VSS (or vPC) pair are balanced. You must configure the `vss-id` keyword in the `channel-group` command for each member interface before enabling load balancing (see Step 2).

**Step 7** (Optional) You can set the Ethernet properties for the port-channel interface to override the properties set on the Individual interfaces.

This method provides a shortcut to set these parameters because these parameters must match for all interfaces in the channel group.

**Step 8** (Optional) If you are creating VLAN subinterfaces on this EtherChannel, do so now.

Example:
```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

The rest of this procedure applies to the subinterfaces.

**Step 9** (Multiple Context Mode) Allocate the interface to a context. Then enter:

```
changeto context name
interface port-channel channel_id
```

Example:
```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

For multiple context mode, the rest of the interface configuration occurs within each context.

**Step 10** Name the interface:

```
nameif name
```

Example:
```
ciscoasa(config-if)# nameif inside
```

The `name` is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value.

**Step 11** Perform one of the following, depending on the firewall mode.

- **Routed Mode**—Set the IPv4 and/or IPv6 address:
  
  (IPv4)
  
  ```
ip address ip_address [mask]
```

  (IPv6)
  
  ```
ipv6 address ipv6-prefix/prefix-length
```

Example:
```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

DHCP, PPPoE, and IPv6 autoconfig are not supported.

- **Transparent Mode**—Assign the interface to a bridge group:
  
  ```
bridge-group number
```
Example:
```bash
ciscoasa(config-if)# bridge-group 1
```

Where `number` is an integer between 1 and 100. You can assign up to four interfaces to a bridge group. You cannot assign the same interface to more than one bridge group. Note that the BVI configuration includes the IP address.

**Step 12** Set the security level:
```
security-level number
```

Example:
```bash
ciscoasa(config-if)# security-level 50
```

Where `number` is an integer between 0 (lowest) and 100 (highest).

**Step 13** Configure a MAC address for a Spanned EtherChannel so that the MAC address does not change when the current master unit leaves the cluster:
```
mac-address mac_address
```

Example:
```bash
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

With a manually-configured MAC address, the MAC address stays with the current master unit. In multiple context mode, if you share an interface between contexts, auto-generation of MAC addresses is enabled by default, so that you only need to set the MAC address manually for a shared interface if you disable auto-generation. Note that you must manually configure the MAC address for non-shared interfaces.

The `mac_address` is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE.

The first two bytes of a manual MAC address cannot be A2 if you also want to use auto-generated MAC addresses.

---

**Related Topics**
- Configure the Cluster Interface Mode on Each Unit, page 8-39
- Configuring Bridge Groups, page 12-7
- Configure the Master Unit Bootstrap Settings, page 8-47
- Configure an EtherChannel, page 9-18
- EtherChannels, page 9-12
- Connecting to a VSS or vPC, page 8-14
- Enable the Physical Interface and Configure Ethernet Parameters, page 9-14
- Configure VLAN Subinterfaces and 802.1Q Trunking, page 9-21
- Configure a Security Context, page 6-19
- Security Levels, page 11-1
- Guidelines for ASA Clustering, page 8-33
Configure the Master Unit Bootstrap Settings

Each unit in the cluster requires a bootstrap configuration to join the cluster. Typically, the first unit you configure to join the cluster will be the master unit. After you enable clustering, after an election period, the cluster elects a master unit. With only one unit in the cluster initially, that unit will become the master unit. Subsequent units that you add to the cluster will be slave units.

Before You Begin

- You must use the console port to enable or disable clustering. You cannot use Telnet or SSH.
- Back up your configurations in case you later want to leave the cluster, and need to restore your configuration.
- For multiple context mode, complete these procedures in the system execution space. To change from the context to the system execution space, enter the **changentoc system** command.
- We recommend enabling jumbo frame reservation for use with the cluster control link.
- With the exception of the cluster control link, any interfaces in your configuration must be configured with a cluster IP pool or as a Spanned EtherChannel before you enable clustering, depending on your interface mode. If you have pre-existing interface configuration, you can either clear the interface configuration (**clear configure interface**), or convert your interfaces to cluster interfaces before you enable clustering.
- When you add a unit to a running cluster, you may see temporary, limited packet/connection drops; this is expected behavior.
- Determine the size of the cluster control link.

Procedure

**Step 1** Enable the cluster control link interface before you join the cluster.

You will later identify this interface as the cluster control link when you enable clustering.

We recommend that you combine multiple cluster control link interfaces into an EtherChannel if you have enough interfaces. The EtherChannel is local to the ASA, and is not a Spanned EtherChannel.

The cluster control link interface configuration is not replicated from the master unit to slave units; however, you must use the same configuration on each unit. Because this configuration is not replicated, you must configure the cluster control link interfaces separately on each unit.

- You cannot use a VLAN subinterface as the cluster control link.
- You cannot use a Management \( x/x \) interface as the cluster control link, either alone or as an EtherChannel.
- For the ASA 5585-X with an ASA IPS module, you cannot use the module interfaces for the cluster control link.

a. Enter interface configuration mode:

```
interface interface_id
```

Example:

```
ciscoasa(config)# interface tengigabitethernet 0/6
```

b. (Optional, for an EtherChannel) Assign this physical interface to an EtherChannel:

```
channel-group channel_id mode on
```
Example:
```plaintext
ciscoasa(config-if)# channel-group 1 mode on
```

The `channel_id` is between 1 and 48. If the port-channel interface for this channel ID does not yet exist in the configuration, one will be added automatically:

```plaintext
interface port-channel channel_id
```

We recommend using the On mode for cluster control link member interfaces to reduce unnecessary traffic on the cluster control link. The cluster control link does not need the overhead of LACP traffic because it is an isolated, stable network. Note: We recommend setting `data` EtherChannels to Active mode.

c. Enable the interface:
   ```plaintext
   no shutdown
   ```

   You only need to enable the interface; do not configure a name for the interface, or any other parameters.

d. (For an EtherChannel) Repeat for each additional interface you want to add to the EtherChannel:
   ```plaintext
   Example:
   ciscoasa(config)# interface tengigabitethernet 0/7
   ciscoasa(config-if)# channel-group 1 mode on
   ciscoasa(config-if)# no shutdown
   ```

**Step 2** (Optional) Specify the maximum transmission unit for the cluster control link interface:

```plaintext
mtu cluster bytes
```

Example:
```plaintext
ciscoasa(config)# mtu cluster 9000
```

Set the MTU between 64 and 65,535 bytes. The default MTU is 1500 bytes.

We suggest setting the MTU to 1600 bytes or greater, which requires you to enable jumbo frame reservation before continuing with this procedure. Jumbo frame reservation requires a reload of the ASA.

This command is a global configuration command, but is also part of the bootstrap configuration that is not replicated between units.

**Step 3** Name the cluster and enter cluster configuration mode:

```plaintext
cluster group name
```

Example:
```plaintext
ciscoasa(config)# cluster group pod1
```

The name must be an ASCII string from 1 to 38 characters. You can only configure one cluster group per unit. All members of the cluster must use the same name.

**Step 4** Name this member of the cluster:

```plaintext
local-unit unit_name
```

```plaintext
ciscoasa(cfg-cluster)# local-unit unit1
```

Use a unique ASCII string from 1 to 38 characters. Each unit must have a unique name. A unit with a duplicated name will be not be allowed in the cluster.
**Step 5** Specify the cluster control link interface, preferably an EtherChannel:

```
cluster-interface interface_id ip ip_address mask
```

Example:

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

Subinterfaces and Management interfaces are not allowed. Specify an IPv4 address for the IP address; IPv6 is not supported for this interface. This interface cannot have a nameif configured.

For each unit, specify a different IP address on the same network.

**Step 6** Set the priority of this unit for master unit elections:

```
priority priority_number
```

Example:

```
ciscoasa(cfg-cluster)# priority 1
```

The priority is between 1 and 100, where 1 is the highest priority.

**Step 7** (Optional) Set an authentication key for control traffic on the cluster control link:

```
key shared_secret
```

Example:

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

The shared secret is an ASCII string from 1 to 63 characters. The shared secret is used to generate the key. This command does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

**Step 8** (Optional) Customize the cluster health check feature, which includes unit health monitoring and interface health monitoring:

```
health-check [holdtime timeout] [vss-enabled]
```

Example:

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

The **holdtime** determines the amount of time between unit keepalive status messages, between .8 and 45 seconds; The default is 3 seconds. Note that the holdtime value only affects the **unit** health check; for interface health, the ASA uses the interface status (up or down).

To determine unit health, the ASA cluster units send keepalive messages on the cluster control link to other units. If a unit does not receive any keepalive messages from a peer unit within the holdtime period, the peer unit is considered unresponsive or dead. If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, then you might need to enable the **vss-enabled** option. 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 **vss-enabled**, 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.
The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular unit, but there are active ports under the same logical interface on other units, then the unit is removed from the cluster. The amount of time before the ASA removes a member from the cluster depends on the type of interface and whether the unit is an established member or is joining the cluster.

Health check is enabled by default. You can disable it using the `no` form of this command.

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the ASA or the switch, or adding an additional switch to form a VSS or vPC) you should disable the health check feature. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the health check feature.

**Step 9**
(Optional) Enable connection rebalancing for TCP traffic:

```plaintext
conn-rebalance [frequency seconds]
```

Example:

```plaintext
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

This command is disabled by default. If enabled, ASAs exchange load information periodically, and offload new connections from more loaded devices to less loaded devices. The frequency, between 1 and 360 seconds, specifies how often the load information is exchanged. The default is 5 seconds.

Do not configure connection rebalancing for inter-site topologies; you do not want connections rebalanced to cluster members at a different site.

**Step 10**
(Optional) Enable console replication from slave units to the master unit:

```plaintext
console-replicate
```

This feature is disabled by default. The ASA prints out some messages directly to the console for certain critical events. If you enable console replication, slave units send the console messages to the master unit so that you only need to monitor one console port for the cluster.

**Step 11**
(Optional) Disable dynamic port priority in LACP:

```plaintext
clacp static-port-priority
```

Some switches do not support dynamic port priority, so this command improves switch compatibility. Moreover, it enables support of more than 8 active spanned EtherChannel members, up to 32 members. Without this command, only 8 active members and 8 standby members are supported. If you enable this command, then you cannot use any standby members; all members are active.

**Step 12**
(Optional) Manually specify the cLACP system ID and system priority:

```plaintext
clacp system-mac (mac_address | auto) [system-priority number]
```

Example:

```plaintext
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

When using Spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch. ASAs in a cluster collaborate in cLACP negotiation so that they appear as a single (virtual) device to the switch. One parameter in cLACP negotiation is a system ID, which is in the format of a MAC address. All ASAs in the cluster use the same system ID: auto-generated by the master unit (the default) and replicated to all slaves; or manually specified in this command in the form H.H.H, where H is a 16-bit hexadecimal digit. (For example, the MAC address 00-0A-00-00-AA-AA is entered as 000A.0000.AAAA.) You might want to manually configure the MAC address for troubleshooting purposes, for example, so that you can use an easily identified MAC address. Typically, you would use the auto-generated MAC address.
The system priority, between 1 and 65535, is used to decide which unit is in charge of making a bundling decision. By default, the ASA uses priority 1, which is the highest priority. The priority needs to be higher than the priority on the switch.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units. However, you cannot change this value after you enable clustering.

**Step 13**

Enable clustering:

```
enable [noconfirm]
```

Example:

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
class inspection_default
inspect skinny
policy-map global_policy
class inspection_default
inspect sip
Would you like to remove these commands? [Y]es/[N]o:Y
INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

When you enter the `enable` command, the ASA scans the running configuration for incompatible commands for features that are not supported with clustering, including commands that may be present in the default configuration. You are prompted to delete the incompatible commands. If you respond **No**, then clustering is not enabled. Use the `noconfirm` keyword to bypass the confirmation and delete incompatible commands automatically.

For the first unit enabled, a master unit election occurs. Because the first unit should be the only member of the cluster so far, it will become the master unit. Do not perform any configuration changes during this period.

To disable clustering, enter the `no enable` command.

**Note** If you disable clustering, all data interfaces are shut down, and only the management-only interface is active.

**Examples**

The following example configures a management interface, configures a device-local EtherChannel for the cluster control link, and then enables clustering for the ASA called “unit1,” which will become the master unit because it is added to the cluster first:

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
interface management 0/0
  nameif management
  ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
  ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
  security-level 100
  management-only
```
Configure ASA Clustering

Chapter 8      ASA Cluster

Configure Slave Unit Bootstrap Settings

Perform the following procedure to configure the slave units.

Before You Begin
- You must use the console port to enable or disable clustering. You cannot use Telnet or SSH.
- Back up your configurations in case you later want to leave the cluster, and need to restore your configuration.
- For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.
- We recommend enabling jumbo frame reservation for use with the cluster control link.
- If you have any interfaces in your configuration that have not been configured for clustering (for example, the default configuration Management 0/0 interface), you can join the cluster as a slave unit (with no possibility of becoming the master in a current election).
- When you add a unit to a running cluster, you may see temporary, limited packet/connection drops; this is expected behavior.

Procedure

Step 1  Configure the same cluster control link interface as you configured for the master unit.

Example:

ciscoasa(config)# interface tengigabitethernet 0/6
ciscoasa(config-if)# channel-group 1 mode on
Step 2  Specify the same MTU that you configured for the master unit:
   Example:
   ```
ciscoasa(config)# mtu cluster 9000
   ```

Step 3  Identify the same cluster name that you configured for the master unit:
   Example:
   ```
ciscoasa(config)# cluster group pod1
   ```

Step 4  Name this member of the cluster with a unique string:
   ```
local-unit  unit_name
   ```
   Example:
   ```
ciscoasa(cfg-cluster)# local-unit unit2
   ```
   Specify an ASCII string from 1 to 38 characters.
   Each unit must have a unique name. A unit with a duplicated name will be not be allowed in the cluster.

Step 5  Specify the same cluster control link interface that you configured for the master unit, but specify a different IP address on the same network for each unit:
   ```
cluster-interface  interface_id  ip  ip_address  mask
   ```
   Example:
   ```
ciscoasa(config)# cluster-interface port-channel2  ip  192.168.1.2  255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
   ```
   Specify an IPv4 address for the IP address; IPv6 is not supported for this interface. This interface cannot have a nameif configured.

Step 6  Set the priority of this unit for master unit elections, typically to a higher value than the master unit:
   ```
priority  priority_number
   ```
   Example:
   ```
ciscoasa(config)# priority 2
   ```
   Set the priority between 1 and 100, where 1 is the highest priority.

Step 7  Set the same authentication key that you set for the master unit:
   Example:
   ```
ciscoasa(config)# key chuntheunavoidable
   ```

Step 8  Enable clustering:
   ```
enable as-slave
   ```
   You can avoid any configuration incompatibilities (primarily the existence of any interfaces not yet configured for clustering) by using the `enable as-slave` command. This command ensures the slave joins the cluster with no possibility of becoming the master in any current election. Its configuration is overwritten with the one synced from the master unit.
   To disable clustering, enter the `no enable` command.
Note
If you disable clustering, all data interfaces are shut down, and only the management interface is active.

Examples
The following example includes the configuration for a slave unit, unit2:

```
interface tengigabitethernet 0/6
  channel-group 1 mode on
  no shutdown

interface tengigabitethernet 0/7
  channel-group 1 mode on
  no shutdown

cluster group pod1
  local-unit unit2
  cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
  priority 2
  key chuntheunavoidable
  enable as-slave
```

Related Topics
- Enable Jumbo Frame Support, page 9-22
- Master Unit Election, page 8-3
- Leave the Cluster, page 8-56
- Change the Master Unit, page 8-57
- Execute a Command Cluster-Wide, page 8-58

Manage ASA Cluster Members

After you deploy the cluster, you can change the configuration and manage cluster members.

- Become an Inactive Member, page 8-54
- Inactivate a Member, page 8-55
- Leave the Cluster, page 8-56
- Change the Master Unit, page 8-57
- Execute a Command Cluster-Wide, page 8-58

Become an Inactive Member

To become an inactive member of the cluster, disable clustering on the unit while leaving the clustering configuration intact.
When an ASA becomes inactive (either manually or through a health check failure), all data interfaces are shut down; only the management-only interface can send and receive traffic. To resume traffic flow, re-enable clustering; or you can remove the unit altogether from the cluster. The management interface remains up using the IP address the unit received from the cluster IP pool. However if you reload, and the unit is still inactive in the cluster, the management interface is not accessible (because it then uses the Main IP address, which is the same as the master unit). You must use the console port for any further configuration.

Before You Begin

- You must use the console port; you cannot enable or disable clustering from a remote CLI connection.
- For multiple context mode, perform this procedure in the system execution space. If you are not already in the System configuration mode, enter the `chargeto system` command.

Procedure

**Step 1** Enter cluster configuration mode:

```
cluster group name
```

Example:

```
ciscoasa(config)# cluster group pod1
```

**Step 2** Disable clustering:

```
no enable
```

If this unit was the master unit, a new master election takes place, and a different member becomes the master unit.

The cluster configuration is maintained, so that you can enable clustering again later.

Related Topics

- Leave the Cluster, page 8-56

Inactivate a Member

To inactivate a member from any unit, perform the following steps.

When an ASA becomes inactive, all data interfaces are shut down; only the management-only interface can send and receive traffic. To resume traffic flow, re-enable clustering; or you can remove the unit altogether from the cluster. The management interface remains up using the IP address the unit received from the cluster IP pool. However if you reload, and the unit is still inactive in the cluster, the management interface is not accessible (because it then uses the Main IP address, which is the same as the master unit). You must use the console port for any further configuration.
**Before You Begin**

For multiple context mode, perform this procedure in the system execution space. If you are not already in the System configuration mode, enter the `changeto system` command.

**Procedure**

### Step 1

Remove the unit from the cluster:

```
cluster remove unit unit_name
```

Example:

```
ciscoasa(config)# cluster remove unit ?
```

Current active units in the cluster:

```
asa2
```

```
ciscoasa(config)# cluster remove unit asa2
```

**WARNING:** Clustering will be disabled on unit asa2. To bring it back to the cluster please logon to that unit and re-enable clustering.

The bootstrap configuration remains intact, as well as the last configuration synced from the master unit, so that you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master unit is elected.

To view member names, enter `cluster remove unit ?`, or enter the `show cluster info` command.

---

**Related Topics**

- Leave the Cluster, page 8-56

---

**Leave the Cluster**

If you want to leave the cluster altogether, you need to remove the entire cluster bootstrap configuration. Because the current configuration on each member is the same (synced from the master unit), leaving the cluster also means either restoring a pre-clustering configuration from backup, or clearing your configuration and starting over to avoid IP address conflicts.

**Before You Begin**

You must use the console port; when you remove the cluster configuration, all interfaces are shut down, including the management interface and cluster control link. Moreover, you cannot enable or disable clustering from a remote CLI connection.

**Procedure**

### Step 1

For a slave unit, disable clustering:

```
cluster group cluster_name
no enable
```

Example:

```
ciscoasa(config)# cluster group cluster1
```

```
ciscoasa(config)# no enable
```

---

8-56
You cannot make configuration changes while clustering is enabled on a slave unit.

**Step 2**  
Clear the cluster configuration:  
```
clear configure cluster
```

The ASA shuts down all interfaces including the management interface and cluster control link.

**Step 3**  
Disable cluster interface mode:  
```
no cluster interface-mode
```

The mode is not stored in the configuration and must be reset manually.

**Step 4**  
If you have a backup configuration, copy the backup configuration to the running configuration:  
```
copy backup_cfg running-config
```

Example:
```
ciscoasa(config)# copy backup_cluster.cfg running-config
```

**Step 5**  
Save the configuration to startup:  
```
write memory
```

**Step 6**  
If you do not have a backup configuration, reconfigure management access. Be sure to change the interface IP addresses, and restore the correct hostname, for example.

---

**Related Topics**
- Chapter 2, “Getting Started.”

---

**Change the Master Unit**

⚠️ **Caution**
The best method to change the master unit is to disable clustering on the master unit, waiting for a new master election, and then re-enabling clustering. If you must specify the exact unit you want to become the master, use the procedure in this section. Note, however, that for centralized features, if you force a master unit change using this procedure, then all connections are dropped, and you have to re-establish the connections on the new master unit.

To change the master unit, perform the following steps.

**Before You Begin**
For multiple context mode, perform this procedure in the system execution space. If you are not already in the System configuration mode, enter the **chargeto system** command.

**Procedure**

**Step 1**  
Set a new unit as the master unit:
**cluster master unit unit_name**

Example:
ciscoasa(config)# cluster master unit asa2

You will need to reconnect to the Main cluster IP address.

To view member names, enter `cluster master unit ?` (to see all names except the current unit), or enter the `show cluster info` command.

---

**Related Topics**
- Become an Inactive Member, page 8-54
- Centralized Features for Clustering, page 8-26

---

**Execute a Command Cluster-Wide**

To send a command to all members in the cluster, or to a specific member, perform the following steps. Sending a `show` command to all members collects all output and displays it on the console of the current unit. Other commands, such as `capture` and `copy`, can also take advantage of cluster-wide execution.

**Procedure**

**Step 1** Send a command to all members, or if you specify the unit name, a specific member:

`cluster exec [unit unit_name] command`

Example:
ciscoasa# cluster exec show xlate

To view member names, enter `cluster exec unit ?` (to see all names except the current unit), or enter the `show cluster info` command.

---

**Examples**

To copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the following command on the master unit:
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as capture1_asa1.pcap, capture1_asa2.pcap, and so on. In this example, asa1 and asa2 are cluster unit names.

The following sample output for the `cluster exec show port-channel` summary command shows EtherChannel information for each member in the cluster:

ciscoasa# cluster exec show port-channel summary
primary(LOCAL):***********************************************************
Number of channel-groups in use: 2
Group Port-channel Protocol Span-cluster Ports
---------------------------------------------------------------
1   Po1      LACP      Yes  Gi0/0(P)
2   Po2      LACP      Yes  Gi0/1(P)
### Monitoring the ASA Cluster

You can monitor and troubleshoot cluster status and connections.

- Monitoring Cluster Status, page 8-59
- Capturing Packets Cluster-Wide, page 8-60
- Monitoring Cluster Resources, page 8-60
- Monitoring Cluster Traffic, page 8-60
- Monitoring Cluster Routing, page 8-63
- Configuring Logging for Clustering, page 8-63
- Monitoring Cluster Interfaces, page 8-63
- Debugging Clustering, page 8-63

#### Monitoring Cluster Status

See the following commands for monitoring cluster status:

- **show cluster info [health]**

  With no keywords, the `show cluster info` command shows the status of all members of the cluster.

  The `show cluster info health` command shows the current health of interfaces, units, and the cluster overall.

  See the following output for the `show cluster info` command:

  ```
ciscoasa# show cluster info
Cluster stbu: On
This is "C" in state SLAVE
   ID : 0
   Version : 100.8(0.52)
   Serial No.: P3000000025
   CCL IP   : 10.0.0.3
   CCL MAC   : 000b.fcf8.c192
   Last join : 17:08:59 UTC Sep 26 2011
   Last leave: N/A
Other members in the cluster:
Unit "D" in state SLAVE
   ID : 1
   Version : 100.8(0.52)
   Serial No.: P3000000001
   CCL IP   : 10.0.0.4
   CCL MAC   : 000b.fcf8.c162
   Last join : 19:13:11 UTC Sep 23 2011
   Last leave: N/A
Unit "A" in state MASTER
   ID : 2
   Version : 100.8(0.52)
```
Monitoring the ASA Cluster

Serial No.: JAB0815R0JY
CCL IP : 10.0.0.1
CCL MAC : 000f.f775.541e
Last join : 19:13:20 UTC Sep 23 2011
Last leave: N/A
Unit "B" in state SLAVE
   ID : 3
   Version : 100.8(0.52)
   Serial No.: P3000000191
   CCL IP : 10.0.0.2
   CCL MAC : 000b.fcf8.c61e
   Last join : 19:13:50 UTC Sep 23 2011
   Last leave: 19:13:36 UTC Sep 23 2011

- show cluster history
  Shows the cluster history.

Capturing Packets Cluster-Wide

See the following commands for capturing packets in a cluster:

```
cluster exec capture
```

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.

Related Topics
- Capture Packets, page 38-1

Monitoring Cluster Resources

See the following commands for monitoring cluster resources:

```
show cluster {cpu | memory | resource} [options]
```

Displays aggregated data for the entire cluster. The `options` available depends on the data type.

Monitoring Cluster Traffic

See the following commands for monitoring cluster traffic:

- `show conn [detail], cluster exec show conn`

  The `show conn` command shows whether a flow is a director, backup, or forwarder flow. Use the `cluster exec show conn` command on any unit to view all connections. This command can show how traffic for a single flow arrives at different ASAs in the cluster. The throughput of the cluster is dependent on the efficiency and configuration of load balancing. This command provides an easy way to view how traffic for a connection is flowing through the cluster, and can help you understand how a load balancer might affect the performance of a flow.

  The following is sample output for the `show conn detail` command:

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
```
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, b - TCP state-bypass or nailed,
C - CTIQBE media, c - cluster centralized,
D - DNS, d - dump, E - outside back connection, F - outside FIN, f -
inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - outside back connection, J - GTP, j - GTP data, K - GTP t3-response
l - incomplete, L - GTP l3-response, M - SMTP data, m - SIP media, n - GUP
O - outbound data, P - inside back connection, p - Phone-proxy TFTP
connection,
q - SQL*Net data, R - outside acknowledged FIN, R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
T - SIP, t - SIP transient, U - up, V - VPN orphan, W - WAAS,
X - inspected by service module,
x - per session, Y - director stub flow, y - backup stub flow,
Z - Scansafe redirection, z - forwarding stub flow

ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, flags c, idle 0s,
uptime 1m21s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255)
Traffic received at interface outside Locally received: 7544 (93 byte/s) Traffic
received at interface NP Identity Ifc Locally received: 0 (0 byte/s) UDP outside:
10.1.227.1/500 NP Identity Ifc: 10.1.226.1/500, flags UIO, idle 0:00:00, bytes 1580,
timeout 2m0s, bytes 0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received at interface outside Locally received: 864 (10
byte/s) Traffic received at interface NP Identity Ifc Locally received: 716 (8 byte/s)

To troubleshoot the connection flow, first see connections on all units by entering the cluster exec
show conn command on any unit. Look for flows that have the following flags: director (Y), backup
(y), and forwarder (z). The following example shows an SSH connection from 172.18.124.187:22
to 192.168.103.131:44727 on all three ASAs; ASA 1 has the z flag showing it is a forwarder for the
connection, ASA3 has the Y flag showing it is the director for the connection, and ASA2 has no
special flags showing it is the owner. In the outbound direction, the packets for this connection enter
the inside interface on ASA2 and exit the outside interface. In the inbound direction, the packets for
this connection enter the outside interface on ASA1 and ASA3, are forwarded over the cluster
control link to ASA2, and then exit the inside interface on ASA2.

ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):***************************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z

ASA2:***************************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO

ASA3:***************************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:03, bytes 0,
flags Y

- show cluster info [conn-distribution | packet-distribution | loadbalance]

The show cluster info conn-distribution and show cluster info packet-distribution commands
show traffic distribution across all cluster units. These commands can help you to evaluate and
adjust the external load balancer.
The `show cluster info loadbalance` command shows connection rebalance statistics.

- `show cluster [access-list | conn | traffic | user-identity | xlate] [options]`

Displays aggregated data for the entire cluster. The `options` available depends on the data type.

See the following output for the `show cluster access-list` command:

ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B, unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0, 0, 0, 0, 0) 0xfee4f4947
access-list 101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access-list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x4e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104) 0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4414a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfe4a
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d

To display the aggregated count of in-use connections for all units, enter:
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
200 in use (cluster-wide aggregated)
cl2(LOCAL):***********************************************************
100 in use, 100 most used
cl1:******************************************************************
100 in use, 100 most used

- `show asp cluster counter`

This command is useful for datapath troubleshooting.

Related Topics
- Connection Roles, page 11-22
Monitoring Cluster Routing

See the following commands for monitoring cluster routing:

- `show route cluster`
- `debug route cluster`

Shows cluster information for routing.

Configuring Logging for Clustering

See the following commands for configuring logging for clustering:

- `logging device-id`

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.

Related Topics
- Include the Device ID in Non-EMBLEM Format Syslog Messages, page 39-16

Monitoring Cluster Interfaces

See the following commands for monitoring cluster interfaces:

- `show cluster interface-mode`
  Shows the cluster interface mode.
- `show port-channel`
  Includes information about whether a port-channel is spanned.
- `show lacp cluster {system-mac | system-id}`
  Shows the cLACP system ID and priority.
- `debug lacp cluster [all | ccp | misc | protocol]`
  Shows debug messages for cLACP.

Debugging Clustering

See the following commands for debugging clustering:

- `debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]`
  Shows debug messages for clustering.
- `show cluster info trace`

The `show cluster info trace` command shows the debug information for further troubleshooting. See the following output for the `show cluster info trace` command:

```
ciscoasa# show cluster info trace
Feb 02 14:19:47.456 [DBG] Receive CCP message: CCP_MSG_LOAD_BALANCE
Feb 02 14:19:47.456 [DBG] Receive CCP message: CCP_MSG_LOAD_BALANCE
```
Examples for ASA Clustering

These examples include all cluster-related ASA configuration for typical deployments.

- Sample ASA and Switch Configuration, page 8-64
- Firewall on a Stick, page 8-67
- Traffic Segregation, page 8-69
- Spanned EtherChannel with Backup Links (Traditional 8 Active/8 Standby), page 8-71

Sample ASA and Switch Configuration

The following sample configurations connect the following interfaces between the ASA and the switch:

<table>
<thead>
<tr>
<th>ASA Interface</th>
<th>Switch Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet 0/2</td>
<td>GigabitEthernet 1/0/15</td>
</tr>
<tr>
<td>GigabitEthernet 0/3</td>
<td>GigabitEthernet 1/0/16</td>
</tr>
<tr>
<td>GigabitEthernet 0/4</td>
<td>GigabitEthernet 1/0/17</td>
</tr>
<tr>
<td>GigabitEthernet 0/5</td>
<td>GigabitEthernet 1/0/18</td>
</tr>
</tbody>
</table>

- ASA Configuration, page 8-64
- Cisco IOS Switch Configuration, page 8-66

ASA Configuration

Interface Mode on Each Unit

```bash
cluster interface-mode spanned force
```

ASA1 Master Bootstrap Configuration

```bash
interface GigabitEthernet0/0
    channel-group 1 mode on
    no shutdown

interface GigabitEthernet0/1
    channel-group 1 mode on
    no shutdown

interface Port-channel1
    description Clustering Interface

cluster group Moya
    local-unit A
    cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
    priority 10
    key emphyri0
```
enable noconfirm

**ASA2 Slave Bootstrap Configuration**

interface GigabitEthernet0/0
c-channel-group 1 mode on
no shutdown
!
interface GigabitEthernet0/1
c-channel-group 1 mode on
no shutdown
!
interface Port-channel1
description Clustering Interface

cluster group Moya
local-unit B
c-cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
priority 11
key emphyri0
enable as-slave

**Master Interface Configuration**

ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
c-channel-group 10 mode active
no shutdown
!
interface GigabitEthernet0/3
c-channel-group 10 mode active
no shutdown
!
interface GigabitEthernet0/4
c-channel-group 11 mode active
no shutdown
!
interface GigabitEthernet0/5
c-channel-group 11 mode active
no shutdown
!
interface Management0/0
management-only
nameif management
ip address 10.53.195.230 cluster-pool mgmt-pool
security-level 100
no shutdown
!
interface Port-channel10
port-channel span-cluster
mac-address aaaa.bbbb.cccc
nameif inside
security-level 100
ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
port-channel span-cluster
mac-address aaaa.dddd.cccc
nameif outside
security-level 0
ip address 209.165.201.1 255.255.255.224
Cisco IOS Switch Configuration

interface GigabitEthernet1/0/15
        switchport access vlan 201
        switchport mode access
        spanning-tree portfast
        channel-group 10 mode active

interface GigabitEthernet1/0/16
        switchport access vlan 201
        switchport mode access
        spanning-tree portfast
        channel-group 10 mode active

interface GigabitEthernet1/0/17
        switchport access vlan 401
        switchport mode access
        spanning-tree portfast
        channel-group 11 mode active

interface GigabitEthernet1/0/18
        switchport access vlan 401
        switchport mode access
        spanning-tree portfast
        channel-group 11 mode active

interface Port-channel10
        switchport access vlan 201
        switchport mode access

interface Port-channel11
        switchport access vlan 401
        switchport mode access
Firewall on a Stick

Data traffic from different security domains are associated with different VLANs, for example, VLAN 10 for the inside network and VLAN 20 for the outside network. Each ASA has a single physical port connected to the external switch or router. Trunking is enabled so that all packets on the physical link are 802.1q encapsulated. The ASA is the firewall between VLAN 10 and VLAN 20.

When using Spanned EtherChannels, all data links are grouped into one EtherChannel on the switch side. If an ASA becomes unavailable, the switch will rebalance traffic between the remaining units.

**Interface Mode on Each Unit**

```
cluster interface-mode spanned force
```

**ASA1 Master Bootstrap Configuration**

```
interface tengigabitethernet 0/8
  no shutdown
description CCL

cluster group cluster1
  local-unit asa1
  cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
  priority 1
  key chuntheunavoidable
  enable noconfirm
```
ASA2 Slave Bootstrap Configuration

interface tengigabitethernet 0/8
  no shutdown
description CCL

cluster group cluster1
  local-unit asa2
  cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
  priority 2
  key chuntheunavoidable
  enable as-slave

ASA3 Slave Bootstrap Configuration

interface tengigabitethernet 0/8
  no shutdown
description CCL

cluster group cluster1
  local-unit asa3
  cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
  priority 3
  key chuntheunavoidable
  enable as-slave

Master Interface Configuration

ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64

interface management 0/0
  nameif management
  ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
  ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
  security-level 100
  management-only
  no shutdown

interface tengigabitethernet 0/9
  channel-group 2 mode active
  no shutdown
interface port-channel 2
  port-channel span-cluster
interface port-channel 2.10
  vlan 10
  nameif inside
  ip address 10.10.10.5 255.255.255.0
  ipv6 address 2001:DB8:1::5/64
  mac-address 000C.F142.4CDE
interface port-channel 2.20
  vlan 20
  nameif outside
  ip address 209.165.201.1 255.255.255.224
  ipv6 address 2001:DB8:2::8/64
  mac-address 000C.F142.5CDE
Traffic Segregation

You may prefer physical separation of traffic between the inside and outside network.

As shown in the diagram above, there is one Spanned EtherChannel on the left side that connects to the inside switch, and the other on the right side to outside switch. You can also create VLAN subinterfaces on each EtherChannel if desired.

**Interface Mode on Each Unit**

```plaintext
cluster interface-mode spanned force
```

**ASA1 Master Bootstrap Configuration**

```plaintext
interface tengigabitethernet 0/6
   channel-group 1 mode on
   no shutdown
interface tengigabitethernet 0/7
   channel-group 1 mode on
   no shutdown
interface port-channel 1
   description CCL
   cluster group cluster1
   local-unit asa1
   cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
   priority 1
   key chuntheunavoidable
   enable noconfirm
```
ASA2 Slave Bootstrap Configuration

interface tengigabitethernet 0/6
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/7
  channel-group 1 mode on
  no shutdown
interface port-channel 1
  description CCL

cluster group cluster1
  local-unit asa2
  cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
  priority 2
  key chuntheunavoidable
  enable as-slave

ASA3 Slave Bootstrap Configuration

interface tengigabitethernet 0/6
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/7
  channel-group 1 mode on
  no shutdown
interface port-channel 1
  description CCL

cluster group cluster1
  local-unit asa3
  cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
  priority 3
  key chuntheunavoidable
  enable as-slave

Master Interface Configuration

ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
  nameif management
  ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
  ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
  security-level 100
  management-only
  no shutdown

interface tengigabitethernet 0/8
  channel-group 2 mode active
  no shutdown
interface port-channel 2
  port-channel span-cluster
  nameif inside
  ip address 10.10.10.5 255.255.255.0
  ipv6 address 2001:DB8::1:5/64
  mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9
  channel-group 3 mode active
  no shutdown
interface port-channel 3
Spanned EtherChannel with Backup Links (Traditional 8 Active/8 Standby)

The maximum number of active ports in a traditional EtherChannel is limited to 8 from the switch side. If you have an 8-ASA cluster, and you allocate 2 ports per unit to the EtherChannel, for a total of 16 ports total, then 8 of them have to be in standby mode. The ASA uses LACP to negotiate which links should be active or standby. If you enable multi-switch EtherChannel using V SS or vPC, you can achieve inter-switch redundancy. On the ASA, all physical ports are ordered first by the slot number then by the port number. In the following figure, the lower ordered port is the “primary” port (for example, GigabitEthernet 0/0), and the other one is the “secondary” port (for example, GigabitEthernet 0/1). You must guarantee symmetry in the hardware connection: all primary links must terminate on one switch, and all secondary links must terminate on another switch if VSS/vPC is used. The following diagram shows what happens when the total number of links grows as more units join the cluster:

The principle is to first maximize the number of active ports in the channel, and secondly keep the number of active primary ports and the number of active secondary ports in balance. Note that when a 5th unit joins the cluster, traffic is not balanced evenly between all units.
Link or device failure is handled with the same principle. You may end up with a less-than-perfect load balancing situation. The following figure shows a 4-unit cluster with a single link failure on one of the units.
There could be multiple EtherChannels configured in the network. The following diagram shows an EtherChannel on the inside and one on the outside. An ASA is removed from the cluster if both primary and secondary links in one EtherChannel fail. This prevents the ASA from receiving traffic from the outside network when it has already lost connectivity to the inside network.

**Interface Mode on Each Unit**

```
cluster interface-mode spanned force
```

**ASA1 Master Bootstrap Configuration**

```
interface tengigabitethernet 0/6
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/7
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/8
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/9
  channel-group 1 mode on
  no shutdown
interface port-channel 1
description CCL
```
cluster group cluster1
  local-unit asa1
  cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
  priority 1
  key chuntheunavoidable
  enable noconfirm

ASA2 Slave Bootstrap Configuration
interface tengigabitethernet 0/6
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/7
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/8
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/9
  channel-group 1 mode on
  no shutdown
interface port-channel 1
  description CCL
cluster group cluster1
  local-unit asa2
  cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
  priority 2
  key chuntheunavoidable
  enable as-slave

ASA3 Slave Bootstrap Configuration
interface tengigabitethernet 0/6
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/7
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/8
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/9
  channel-group 1 mode on
  no shutdown
interface port-channel 1
  description CCL
cluster group cluster1
  local-unit asa3
  cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
  priority 3
  key chuntheunavoidable
  enable as-slave

ASA4 Slave Bootstrap Configuration
interface tengigabitethernet 0/6
  channel-group 1 mode on
no shutdown
interface tengigabitethernet 0/7
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/8
  channel-group 1 mode on
  no shutdown
interface tengigabitethernet 0/9
  channel-group 1 mode on
  no shutdown
interface port-channel 1
  description CCL

cluster group cluster1
  local-unit asa4
  cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
  priority 4
  key chuntheunavoidable
  enable as-slave

Master Interface Configuration
ip local pool mgmt 10.1.1.2-10.1.1.9
interface management 0/0
  channel-group 2 mode active
  no shutdown
interface management 0/1
  channel-group 2 mode active
  no shutdown
interface port-channel 2
  nameif management
  ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
  security-level 100
  management-only
interface tengigabitethernet 1/6
  channel-group 3 mode active vss-id 1
  no shutdown
interface tengigabitethernet 1/7
  channel-group 3 mode active vss-id 2
  no shutdown
interface port-channel 3
  port-channel span-cluster vss-load-balance
  nameif inside
  ip address 10.10.10.5 255.255.255.0
  mac-address 000C.F142.4CDE
interface tengigabitethernet 1/8
  channel-group 4 mode active vss-id 1
  no shutdown
interface tengigabitethernet 1/9
  channel-group 4 mode active vss-id 2
  no shutdown
interface port-channel 4
  port-channel span-cluster vss-load-balance
  nameif outside
  ip address 209.165.201.1 255.255.255.224
  mac-address 000C.F142.5CDE
History for ASA Clustering

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA Clustering for the ASA 5580 and 5585-X</td>
<td>9.0(1)</td>
<td>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 commands: channel-group, clacp system-mac, clear cluster info, clear configure cluster, cluster exec, cluster group, cluster interface-mode, cluster-interface, conn-rebalance, console-replicate, cluster master unit, cluster remove unit, debug cluster, debug lacp cluster, enable (cluster group), health-check, ip address, ipv6 address, key (cluster group), local-unit, mac-address (interface), mac-address pool, mtu cluster, port-channel span-cluster, priority (cluster group), prompt cluster-unit, show asp cluster counter, show asp table cluster cach-table, show cluster, show cluster info, show cluster user-identity, show lacp cluster, and show running-config cluster.</td>
</tr>
<tr>
<td>ASA 5500-X support for clustering</td>
<td>9.1(4)</td>
<td>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. We did not modify any commands.</td>
</tr>
<tr>
<td>Improved VSS and vPC support for health check monitoring</td>
<td>9.1(4)</td>
<td>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, such as the Cisco Nexus 5000, 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. We modified the following command: health-check [vss-enabled]</td>
</tr>
<tr>
<td>Support for cluster members at different geographical locations (inter-site); Individual Interface mode only</td>
<td>9.1(4)</td>
<td>You can now place cluster members at different geographical locations when using Individual Interface mode. We did not modify any commands.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Support for cluster members at different geographical locations (inter-site) for transparent mode</td>
<td>9.2(1)</td>
<td>You can now place cluster members at different geographical locations when using Spanned EtherChannel mode in transparent firewall mode. Inter-site clustering with spanned EtherChannels in routed firewall mode is not supported. We did not modify any commands.</td>
</tr>
</tbody>
</table>
| Static LACP port priority support for clustering | 9.2(1) | Some switches do not support dynamic port priority with LACP (active and standby links). You can now disable dynamic port priority to provide better compatibility with spanned EtherChannels. You should also follow these guidelines:  
- Network elements on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.  
- Port-channel bundling downtime should not exceed the configured keepalive interval.  
We introduced the following command: `clacp static-port-priority`. |
| Support for 32 active links in a spanned EtherChannel | 9.2(1) | ASA EtherChannels now support up to 16 active links. With *spanned* EtherChannels, that functionality is extended to support up to 32 active links across the cluster when used with two switches in a vPC and when you disable dynamic port priority. The switches must support EtherChannels with 16 active links, for example, the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module.  
For switches in a VSS or vPC that support 8 active links, you can now configure 16 active links in the spanned EtherChannel (8 connected to each switch). Previously, the spanned EtherChannel only supported 8 active links and 8 standby links, even for use with a VSS/vPC.  
**Note** If you want to use more than 8 active links in a spanned EtherChannel, you cannot also have standby links; the support for 9 to 32 active links requires you to disable cLACP dynamic port priority that allows the use of standby links.  
We introduced the following command: `clacp static-port-priority`. |
| Support for 16 cluster members for the ASA 5585-X | 9.2(1) | The ASA 5585-X now supports 16-unit clusters.  
We did not modify any commands. |
We added support for BGP with ASA clustering.
We introduced the following new command: `bgp router-id clusterpool`

You can now deploy a cluster in transparent mode between inside networks and the gateway router at each site (AKA East-West insertion), and extend the inside VLANs between sites. We recommend using Overlay Transport Virtualization (OTV), but you can use any method that ensures that the overlapping MAC Addresses and IP addresses of the gateway router do not leak between sites. Use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide the same virtual MAC and IP addresses to the gateway routers.
PART 3

Interfaces
This chapter includes tasks for starting your interface configuration for the Cisco ASA appliances, including configuring Ethernet settings, redundant interfaces, and EtherChannels.

For multiple context mode, complete all tasks in this section in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.

For ASA cluster interfaces, which have special requirements, see Chapter 8, “ASA Cluster.”

- About Starting ASA Appliance Interface Configuration, page 9-1
- Licensing for ASA Appliance Interfaces, page 9-10
- Guidelines for ASA Appliance Interfaces, page 9-11
- Default Settings for ASA Appliance Interfaces, page 9-13
- Start Interface Configuration (ASA Appliances), page 9-14
- Monitoring Interfaces, page 9-23
- Examples for ASA Appliance Interfaces, page 9-24
- History for ASA Appliance Interfaces, page 9-25
- History for ASA Appliance Interfaces, page 9-25

### About Starting ASA Appliance Interface Configuration

This section describes interface features and special interfaces.

- Auto-MDI/MDIX Feature, page 9-2
- Interfaces in Transparent Mode, page 9-2
- Management Interface, page 9-2
- Redundant Interfaces, page 9-4
- EtherChannels, page 9-5
- Control Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size, page 9-7
Auto-MDI/MDIX Feature

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

Interfaces in Transparent Mode

Interfaces in transparent mode belong to a “bridge group,” one bridge group for each network. You can have up to 8 bridge groups of 4 interfaces each per context or in single mode.

Related Topics
- Bridge Groups in Transparent Mode, page 12-1

Management Interface

The management interface, depending on your model, is a separate interface just for management traffic.

- Management Interface Overview, page 9-2
- Management Slot/Port Interface, page 9-3
- Use Any Interface for Management-Only Traffic, page 9-3
- Management Interface for Transparent Mode, page 9-3
- No Support for Redundant Management Interfaces, page 9-4
- Management Interface on the ASA 5555-X and Lower, page 9-4

Management Interface Overview

You can manage the ASA by connecting to:

- Any through-traffic interface
- A dedicated Management Slot/Port interface (if available for your model)

You may need to configure management access to the interface according to Chapter 35, “Management Access.”
Management **Slot/Port Interface**

The following table shows the Management interfaces per model.

**Table 9-1 Management Interfaces Per Model**

<table>
<thead>
<tr>
<th>Model</th>
<th>Management 0/0</th>
<th>Management 0/1</th>
<th>Management 1/0</th>
<th>Management 1/1</th>
<th>Configurable for Through Traffic</th>
<th>Subinterfaces Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ASA 5585-X</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note**
If you installed a module, then the module management interface(s) provides management access for the module only. For models with software modules, the software module uses the same physical Management interface as the ASA.

**Use Any Interface for Management-Only Traffic**

You can use any interface as a dedicated management-only interface by configuring it for management traffic, including an EtherChannel interface (see the `management-only` command).

**Management Interface for Transparent Mode**

In transparent firewall mode, in addition to the maximum allowed through-traffic interfaces, you can also use the Management interface (either the physical interface, a subinterface (if supported for your model), or an EtherChannel interface comprised of Management interfaces (if you have multiple Management interfaces)) as a separate management interface. You cannot use any other interface types as management interfaces.
Chapter 9    Basic Interface Configuration (ASA Appliances)

In multiple context mode, you cannot share any interfaces, including the Management interface, across contexts. To provide management per context, you can create subinterfaces of the Management interface and allocate a Management subinterface to each context. Note that the ASA 5555-X and lower do not allow subinterfaces on the Management interface, so for per-context management, you must connect to a data interface.

The management interface is not part of a normal bridge group. Note that for operational purposes, it is part of a non-configurable bridge group.

Note

In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the ASA updates the MAC address table to use the management interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the ASA will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.

No Support for Redundant Management Interfaces

Redundant interfaces do not support Management slot/port interfaces as members. You also cannot set a redundant interface comprised of non-Management interfaces as management-only.

Management Interface on the ASA 5555-X and Lower

The Management interface on the ASA 5555-X and lower has the following characteristics:

- No through traffic support
- No subinterface support
- No priority queue support
- No multicast MAC support
- The software module shares the Management interface. Separate MAC addresses and IP addresses are supported for the ASA and module. You must perform configuration of the module IP address within the module operating system. However, physical characteristics (such as enabling the interface) are configured on the ASA.

Redundant Interfaces

A logical redundant interface consists of a pair of physical interfaces: an active and a standby 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 device-level failover if desired.
Redundant Interface MAC Address

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses. When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Related Topics
- Configuring the MAC Address, MTU, and TCP MSS, page 11-9
- Configure Multiple Contexts, page 6-14

EtherChannels

An 802.3ad EtherChannel is a logical interface (called a port-channel interface) consisting of a bundle of individual Ethernet links (a channel group) so that you increase the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels.
- Channel Group Interfaces, page 9-5
- Connecting to an EtherChannel on Another Device, page 9-5
- Link Aggregation Control Protocol, page 9-6
- Load Balancing, page 9-7
- EtherChannel MAC Address, page 9-7

Channel Group Interfaces

Each channel group can have up to 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure. For 16 active interfaces, be sure that your switch supports the feature (for example, the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module).

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

The EtherChannel aggregates the traffic across all the available active interfaces in the channel. The interface is selected using a proprietary hash algorithm, based on source or destination MAC addresses, IP addresses, TCP and UDP port numbers and VLAN numbers.

Connecting to an EtherChannel on Another Device

The device to which you connect the ASA EtherChannel must also support 802.3ad EtherChannels; for example, you can connect to the Catalyst 6500 switch or the Cisco Nexus 7000.

When the switch is part of a Virtual Switching System (VSS) or Virtual Port Channel (vPC), then you can connect ASA interfaces within the same EtherChannel to separate switches in the VSS/vPC. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch.
If you use the ASA in an Active/Standby failover deployment, then you need to create separate EtherChannels on the switches in the VSS/vPC, one for each ASA. On each ASA, a single EtherChannel connects to both switches. Even if you could group all switch interfaces into a single EtherChannel connecting to both ASAs (in this case, the EtherChannel will not be established because of the separate ASA system IDs), a single EtherChannel would not be desirable because you do not want traffic sent to the standby ASA.

**Figure 9-2  Active/Standby Failover and VSS/vPC**

---

### Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

You can configure each physical interface in an EtherChannel to be:

- **Active**—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- **Passive**—Receives LACP updates. A passive EtherChannel can only establish connectivity with an active EtherChannel.
• On—The EtherChannel is always on, and LACP is not used. An “on” EtherChannel can only establish a connection with another “on” EtherChannel.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

**Load Balancing**

The ASA distributes packets to the interfaces in the EtherChannel by hashing the source and destination IP address of the packet (this criteria is configurable). The resulting hash is divided by the number of active links in a modulo operation where the resulting remainder determines which interface owns the flow. All packets with a hash_value mod active_links result of 0 go to the first interface in the EtherChannel, packets with a result of 1 go to the second interface, packets with a result of 2 go to the third interface, and so on. For example, if you have 15 active links, then the modulo operation provides values from 0 to 14. For 6 active links, the values are 0 to 5, and so on.

For a spanned EtherChannel in clustering, load balancing occurs on a per ASA basis. For example, if you have 32 active interfaces in the spanned EtherChannel across 8 ASAs, with 4 interfaces per ASA in the EtherChannel, then load balancing only occurs across the 4 interfaces on the ASA.

If an active interface goes down and is not replaced by a standby interface, then traffic is rebalanced between the remaining links. The failure is masked from both Spanning Tree at Layer 2 and the routing table at Layer 3, so the switchover is transparent to other network devices.

**Related Topics**

• Customize the EtherChannel, page 9-20

**EtherChannel MAC Address**

All interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links.

The port-channel interface uses the lowest numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can manually configure a MAC address for the port-channel interface. In multiple context mode, you can automatically assign unique MAC addresses to interfaces, including an EtherChannel port interface. We recommend manually, or in multiple context mode, automatically configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.

**Control Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size**

Setting the correct MTU and maximum TCP segment size is essential for the best network performance.

• MTU Overview, page 9-8
• Default MTU, page 9-8
• Path MTU Discovery, page 9-8
About Starting ASA Appliance Interface Configuration

- Set the MTU and Jumbo Frames, page 9-8
- TCP Maximum Segment Size Overview, page 9-9
- Default TCP MSS, page 9-9
- Set the TCP MSS for VPN and Non-VPN Traffic, page 9-9
- Examples, page 9-9

MTU Overview

The maximum transmission unit (MTU) specifies the maximum frame payload size that the ASA can transmit on a given Ethernet interface. The MTU value is the frame size without Ethernet headers, FCS, or VLAN tagging. The Ethernet header is 14 bytes and the FCS is 4 bytes. When you set the MTU to 1500, the expected frame size is 1518 bytes including the headers. If you are using VLAN tagging (which adds an additional 4 bytes), then when you set the MTU to 1500, the expected frame size is 1522. Do not set the MTU value higher to accommodate these headers. For information about accommodating TCP headers for encapsulation, do not alter the MTU setting; instead change the TCP Maximum Segment Size.

If an outgoing IP packet is larger than the specified MTU, it is fragmented into 2 or more frames. Fragments are reassembled at the destination (and sometimes at intermediate hops), and fragmentation can cause performance degradation. Therefore, your IP packets should fit within the MTU size to avoid fragmentation.

**Note**
The ASA can receive frames larger than the configured MTU as long as there is room in memory.

Related Topics
- TCP Maximum Segment Size Overview, page 9-9
- Enable Jumbo Frame Support, page 9-22

Default MTU

The default MTU on the ASA is 1500 bytes. This value does not include the 18 or more bytes for the Ethernet header, CRC, VLAN tagging, and so on.

Path MTU Discovery

The ASA supports Path MTU Discovery (as defined in RFC 1191), which lets all devices in a network path between two hosts coordinate the MTU so they can standardize on the lowest MTU in the path.

Set the MTU and Jumbo Frames

See Configuring the MAC Address, MTU, and TCP MSS, page 11-9. For multiple context mode, set the MTU within each context.

See Enable Jumbo Frame Support, page 9-22. For multiple context mode, set the jumbo frame support in the system execution space.
See the following guidelines:

- Matching MTUs on the traffic path—We recommend that you set the MTU on all ASA interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.
- Accommodating jumbo frames—If you enable jumbo frames, you can set the MTU up to 9198 bytes.

TCP Maximum Segment Size Overview

The TCP maximum segment size (TCP MSS) is the size of the TCP payload before any TCP headers are added. UDP packets are not affected. The client and the server exchange TCP MSS values during the three-way handshake when establishing the connection.

You can set the TCP MSS on the ASA. If either endpoint of a connection requests a TCP MSS that is larger than the value set on the ASA, the ASA overwrites the TCP MSS in the request packet with the ASA maximum. If the host or server does not request a TCP MSS, then the ASA assumes the RFC 793-default value of 536 bytes, but does not modify the packet. You can also configure the minimum TCP MSS; if a host or server requests a very small TCP MSS, the ASA can adjust the value up. By default, the minimum TCP MSS is not enabled.

For example, you configure the default MTU of 1500 bytes. A host requests an MSS of 1700. If the ASA maximum TCP MSS is 1380, then the ASA changes the MSS value in the TCP request packet to 1380. The server then sends 1380-byte packets.

Default TCP MSS

By default, the maximum TCP MSS on the ASA is 1380 bytes. This default accommodates VPN connections where the headers can add up to 120 bytes; this value fits within the default MTU of 1500 bytes.

Set the TCP MSS for VPN and Non-VPN Traffic

See Configuring the MAC Address, MTU, and TCP MSS, page 11-9. For multiple context mode, set the TCP MSS within each context.

See the following guidelines:

- Non-VPN traffic—If you do not use VPN and do not need extra space for headers, then you should disable the TCP MSS limit and accept the value established between connection endpoints. Because connection endpoints typically derive the TCP MSS from the MTU, non-VPN packets usually fit this TCP MSS.
- VPN traffic—Set the maximum TCP MSS to the MTU - 120. For example, if you use jumbo frames and set the MTU to a higher value, then you need to set the TCP MSS to accommodate the new MTU.

Examples

The following example enables jumbo frames, increases the MTU on all interfaces, and disables the TCP MSS for non-VPN traffic (by setting the TCP MSS to 0, which means there is no limit):

```
  jumbo frame-reservation
  mtu inside 9198
  mtu outside 9198
  sysopt connection tcpmss 0
```
The following example enables jumbo frames, increases the MTU on all interfaces, and changes the TCP MSS for VPN traffic to 9078 (the MTU minus 120):

```plaintext
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

## Licensing for ASA Appliance Interfaces

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 5</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 30</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 536</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 636</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 50</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 716</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 916</td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 916</td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 200</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1316</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 300</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1716</td>
</tr>
</tbody>
</table>
Guidelines for ASA Appliance Interfaces

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5555-X</td>
<td>VLANs: Base License: 500 Interfaces of all types: Base License: 2516</td>
</tr>
<tr>
<td>ASA 5585-X</td>
<td>VLANs: Base and Security Plus License: 1024 Interface Speed for SSP-10 and SSP-20: Base License—1-Gigabit Ethernet for fiber interfaces 10 GE I/O License (Security Plus)—10-Gigabit Ethernet for fiber interfaces (SSP-40 and SSP-60 support 10-Gigabit Ethernet by default.) Interfaces of all types: Base and Security Plus License: 4612</td>
</tr>
</tbody>
</table>

Note

For an interface to count against the VLAN limit, you must assign a VLAN to it. For example:
```bash
interface gigabitethernet 0/0.100
vlan 100
```

Interfaces of all types comprise the maximum number of combined interfaces; for example, VLANs, physical, redundant, bridge group, and EtherChannel interfaces. Every interface command defined in the configuration counts against this limit. For example, both of the following interfaces count even if the GigabitEthernet 0/0 interface is defined as part of port-channel 1:
```bash
interface gigabitethernet 0/0
interface port-channel 1
```

Guidelines for ASA Appliance Interfaces

Firewall Mode
- For transparent mode, you can configure up to 8 bridge groups per context or for a single mode device.
- Each bridge group can include up to 4 interfaces.
- For multiple context, transparent mode, each context must use different interfaces; you cannot share an interface across contexts.

Failover
- When you use a redundant or EtherChannel interface as a failover link, it must be pre-configured on both units in the failover pair; you cannot configure it on the primary unit and expect it to replicate to the secondary unit because the failover link itself is required for replication.
- If you use a redundant or EtherChannel interface for the state link, no special configuration is required; the configuration can replicate from the primary unit as normal.
• You can monitor redundant or EtherChannel interfaces for failover using the `monitor-interface` command; be sure to reference the logical redundant interface name. When an active member interface fails over to a standby interface, this activity does not cause the redundant or EtherChannel interface to appear to be failed when being monitored for device-level failover. Only when all physical interfaces fail does the redundant or EtherChannel interface appear to be failed (for an EtherChannel interface, the number of member interfaces allowed to fail is configurable).

• If you use an EtherChannel interface for a failover or state link, then to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a failover link. To alter the configuration, you need to either shut down the EtherChannel while you make changes, or temporarily disable failover; either action prevents failover from occurring for the duration.
• You cannot share a failover or state interface with a data interface.

**Clustering**

• When you use a redundant or EtherChannel interface as the cluster control link, it must be pre-configured on all units in the cluster; you cannot configure it on the primary unit and expect it to replicate to member units because the cluster control link itself is required for replication.

To configure a spanned EtherChannel or an individual cluster interface, see the clustering chapter.

**Redundant Interfaces**

• You can configure up to 8 redundant interface pairs.
• All ASA configuration refers to the logical redundant interface instead of the member physical interfaces.
• You cannot use a redundant interface as part of an EtherChannel, nor can you use an EtherChannel as part of a redundant interface. You cannot use the same physical interfaces in a redundant interface and an EtherChannel interface. You can, however, configure both types on the ASA if they do not use the same physical interfaces.
• If you shut down the active interface, then the standby interface becomes active.
• Redundant interfaces do not support Management `slotport` interfaces as members. You also cannot set a redundant interface comprised of non-Management interfaces as management-only.

**EtherChannels**

• You can configure up to 48 EtherChannels.
• Each channel group can have up to 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group; while only eight interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.
• All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.
• The device to which you connect the ASA EtherChannel must also support 802.3ad EtherChannels; for example, you can connect to the Catalyst 6500 switch or Cisco Nexus 7000 switch.
• The ASA does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS `vlan dot1Q tag native` command, then the ASA will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch. In multiple context mode, these messages are not included in a packet capture, so that you cannot diagnose the issue easily.
The ASA does not support connecting an EtherChannel to a switch stack. If the ASA EtherChannel is connected cross stack, and if the Master switch is powered down, then the EtherChannel connected to the remaining switch will not come up.

All ASA configuration refers to the logical EtherChannel interface instead of the member physical interfaces.

You cannot use a redundant interface as part of an EtherChannel, nor can you use an EtherChannel as part of a redundant interface. You cannot use the same physical interfaces in a redundant interface and an EtherChannel interface. You can, however, configure both types on the ASA if they do not use the same physical interfaces.

**Additional Guidelines**

Some management-related services are not available until a non-management interface is enabled, and the ASA achieves a “System Ready” state. The ASA generates the following syslog message when it is in a “System Ready” state:

```
%ASA-6-199002: Startup completed. Beginning operation.
```

## Default Settings for ASA Appliance Interfaces

This section lists default settings for interfaces if you do not have a factory default configuration.

### Default State of Interfaces

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.
- EtherChannel port-channel interfaces—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.

### Default Speed and Duplex

- By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.
- For fiber interfaces for the 5585-X, the speed is set for automatic link negotiation.

### Default Connector Type

Some models include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default. You can configure the ASA to use the fiber SFP connectors.

### Default MAC Addresses

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.
Start Interface Configuration (ASA Appliances)

To start configuring interfaces, perform the following steps:

**Step 1** (Multiple context mode) Complete all tasks in this section in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.

**Step 2** Enable the Physical Interface and Configure Ethernet Parameters, page 9-14.

Physical interfaces are disabled by default.

**Step 3** (Optional) Configure a Redundant Interface, page 9-16.

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.

**Step 4** (Optional) Configure an EtherChannel, page 9-18.

An EtherChannel groups multiple Ethernet interfaces into a single logical interface.

**Step 5** (Optional) See Configure VLAN Subinterfaces and 802.1Q Trunking, page 9-21.

**Step 6** (Optional) Enable Jumbo Frame Support, page 9-22.

**Step 7** (Multiple context mode only) To complete the configuration of interfaces in the system execution space, perform the following tasks that are documented in Chapter 6, “Multiple Context Mode”:

- To assign interfaces to contexts, see Configure a Security Context, page 6-19.
- (Optional) To automatically assign unique MAC addresses to context interfaces, see Assign MAC Addresses to Context Interfaces Automatically, page 6-23.

The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. Alternatively, you can manually assign MAC addresses within the context according to Configuring the MAC Address, MTU, and TCP MSS, page 11-9.

**Step 8** Complete the interface configuration according to Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”

Enable the Physical Interface and Configure Ethernet Parameters

This section describes how to:

- Enable the physical interface
- Set a specific speed and duplex (if available)
- Enable pause frames for flow control

**Before You Begin**

For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.

**Procedure**

**Step 1** Specify the interface you want to configure:
**interface physical_interface**

Example:
```
ciscoasa(config)# interface gigabitethernet 0/0
```

The **physical_interface** ID includes the type, slot, and port number as *type[slot]port*.

The physical interface types include the following:
- **gigabitethernet**
- **tengigabitethernet**
- **management**

Enter the type followed by *slot/port*, for example, **gigabitethernet0/1**. A space is optional between the type and the slot/port.

**Step 2** (Optional) Set the media type to SFP, if available for your model:
```
media-type sfp
```
To restore the default RJ-45, enter the **media-type rj45** command.

**Step 3** (Optional) Set the speed:
```
speed {auto | 10 | 100 | 1000 | nonegotiate}
```
Example:
```
ciscoasa(config-if)# speed 100
```
For RJ-45 interfaces, the default setting is **auto**.

For SFP interfaces, the default setting is **no speed nonegotiate**, which sets the speed to the maximum speed and enables link negotiation for flow-control parameters and remote fault information. The **nonegotiate** keyword is the only keyword available for SFP interfaces. The **speed nonegotiate** command disables link negotiation.

**Step 4** (Optional) Set the duplex for RJ-45 interfaces:
```
duplex {auto | full | half}
```
Example:
```
ciscoasa(config-if)# duplex full
```
The **auto** setting is the default. The duplex setting for an EtherChannel interface must be **full** or **auto**.

**Step 5** (Optional) Enable pause (XOFF) frames for flow control on GigabitEthernet and TenGigabitEthernet interfaces:
```
flowcontrol send on [low_water high_water pause_time] [noconfirm]
```
Example:
```
ciscoasa(config-if)# flowcontrol send on 95 200 10000
```
If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue. Pause (XOFF) and XON frames are generated automatically by the NIC hardware based on the FIFO buffer usage. A pause frame is sent when the buffer usage exceeds the high-water mark. The default **high_water** value is 128 KB (10 GigabitEthernet) and 24 KB (1 GigabitEthernet); you can set it between 0 and 511 (10 GigabitEthernet) or 0 and 47 KB (1 GigabitEthernet). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark. By default, the...
low_water value is 64 KB (10 GigabitEthernet) and 16 KB (1 GigabitEthernet); you can set it between 0 and 511 (10 GigabitEthernet) or 0 and 47 KB (1 GigabitEthernet). The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by the timer value in the pause frame. The default pause_time value is 26624; you can set it between 0 and 65535. If the buffer usage is consistently above the high-water mark, pause frames are sent repeatedly, controlled by the pause refresh threshold value.

When you use this command, you see the following warning:

Changing flow-control parameters will reset the interface. Packets may be lost during the reset.
Proceed with flow-control changes?

To change the parameters without being prompted, use the noconfirm keyword.

**Note**
Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

**Step 6**
Enable the interface:

```
ciscoasa(config-if)# no shutdown
```

To disable the interface, enter the shutdown command. If you enter the shutdown command, you also shut down all subinterfaces. If you shut down an interface in the system execution space, then that interface is shut down in all contexts that share it.

---

**Configure a Redundant Interface**

A logical redundant interface consists of a pair of physical interfaces: an active and a standby 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.

This section describes how to configure redundant interfaces.

- Configure a Redundant Interface, page 9-16
- Change the Active Interface, page 9-18

---

**Configure a Redundant Interface**

This section describes how to create a redundant interface. By default, redundant interfaces are enabled.

**Before You Begin**

- You can configure up to 8 redundant interface pairs.
- Redundant interface delay values are configurable, but by default the ASA inherits the default delay values based on the physical type of its member interfaces.
- Both member interfaces must be of the same physical type. For example, both must be GigabitEthernet.
• You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the `no nameif` command.

• For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.

Caution

If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

Procedure

Step 1

Add the logical redundant interface:

```
interface redundant number
```

Example:

```
ciscoasa(config)# interface redundant 1
```

The `number` argument is an integer between 1 and 8.

You need to add at least one member interface to the redundant interface before you can configure logical parameters for it such as a name.

Step 2

Add the first member interface to the redundant interface:

```
member-interface physical_interface
```

Example:

```
ciscoasa(config-if)# member-interface gigabitethernet 0/0
```

Redundant interfaces do not support Management `slot/port` interfaces as members.

After you add the interface, any configuration for it (such as an IP address) is removed.

Step 3

Add the second member interface to the redundant interface:

```
member-interface physical_interface
```

Example:

```
ciscoasa(config-if)# member-interface gigabitethernet 0/1
```

Make sure the second interface is the same physical type as the first interface.

To remove a member interface, enter the `no member-interface physical_interface` command. You cannot remove both member interfaces from the redundant interface; the redundant interface requires at least one member interface.

Examples

The following example creates two redundant interfaces:

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```
Change the Active Interface

By default, the active interface is the first interface listed in the configuration, if it is available.

Procedure

Step 1  To view which interface is active, enter the following command:

ciscoasa# show interface redundantnumber detail | grep Member

Example:

ciscoasa# show interface redundant1 detail | grep Member
Members GigabitEthernet0/3(Active), GigabitEthernet0/2

Step 2  Change the active interface:

ciscoasa# redundant-interface redundantnumber active-member physical_interface

The redundantnumber argument is the redundant interface ID, such as redundant1. The physical_interface is the member interface ID that you want to be active.

Configure an EtherChannel

This section describes how to create an EtherChannel port-channel interface, assign interfaces to the EtherChannel, and customize the EtherChannel.

- Add Interfaces to the EtherChannel, page 9-18
- Customize the EtherChannel, page 9-20

Add Interfaces to the EtherChannel

This section describes how to create an EtherChannel port-channel interface and assign interfaces to the EtherChannel. By default, port-channel interfaces are enabled.

Before You Begin

- You can configure up to 48 EtherChannels.
- Each channel group can have up to 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only eight interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.
- To configure a spanned EtherChannel for clustering, see the clustering chapter instead of this procedure.
- All interfaces in the channel group must be the same type, speed, and duplex. Half duplex is not supported.
- You cannot add a physical interface to the channel group if you configured a name for it. You must first remove the name using the no nameif command.
- For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the changeto system command.
Caution

If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

Procedure

Step 1

Specify the interface you want to add to the channel group:

```
interface physical_interface
```

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
```

The `physical_interface` ID includes the type, slot, and port number as `type[slot]port`. This first interface in the channel group determines the type and speed for all other interfaces in the group.

In transparent mode, if you create a channel group with multiple Management interfaces, then you can use this EtherChannel as the management-only interface.

Step 2

Assign this physical interface to an EtherChannel:

```
channel-group channel_id mode {active | passive | on}
```

Example:

```
ciscoasa(config-if)# channel-group 1 mode active
```

The `channel_id` is an integer between 1 and 48. If the port-channel interface for this channel ID does not yet exist in the configuration, one will be added:

```
interface port-channel channel_id
```

We recommend using `active` mode.

Step 3

(Optional) Set the priority for a physical interface in the channel group:

```
lacp port-priority number
```

Example:

```
ciscoasa(config-if)# lacp port-priority 12345
```

The priority `number` is an integer between 1 and 65535. The default is 32768. The higher the number, the lower the priority. The ASA uses this setting to decide which interfaces are active and which are standby if you assign more interfaces than can be used. If the port priority setting is the same for all interfaces, then the priority is determined by the interface ID (slot/port). The lowest interface ID is the highest priority. For example, GigabitEthernet 0/0 is a higher priority than GigabitEthernet 0/1.

If you want to prioritize an interface to be active even though it has a higher interface ID, then set this command to have a lower value. For example, to make GigabitEthernet 1/3 active before GigabitEthernet 0/7, then make the `lacp port-priority` value be 12345 on the 1/3 interface vs. the default 32768 on the 0/7 interface.

If the device at the other end of the EtherChannel has conflicting port priorities, the system priority is used to determine which port priorities to use. See the `lacp system-priority` command.

Step 4

Repeat Steps 1 through 3 for each interface you want to add to the channel group.
Each interface in the channel group must be the same type and speed. Half duplex is not supported. If you add an interface that does not match, it will be placed in a suspended state.

**Related Topics**
- Link Aggregation Control Protocol, page 9-6
- Customize the EtherChannel, page 9-20

**Customize the EtherChannel**

This section describes how to set the maximum number of interfaces in the EtherChannel, the minimum number of operating interfaces for the EtherChannel to be active, the load balancing algorithm, and other optional parameters.

**Procedure**

**Step 1** Specify the port-channel interface:

```
interface port-channel channel_id
```

Example:

```
ciscoasa(config)# interface port-channel 1
```

This interface was created automatically when you added an interface to the channel group. If you have not yet added an interface, then this command creates the port-channel interface.

You need to add at least one member interface to the port-channel interface before you can configure logical parameters for it such as a name.

**Step 2** Specify the maximum number of active interfaces allowed in the channel group:

```
lacp max-bundle number
```

Example:

```
ciscoasa(config-if)# lacp max-bundle 6
```

The *number* is between 1 and 16. The default is 16. If your switch does not support 16 active interfaces, be sure to set this command to 8 or fewer.

**Step 3** Specify the minimum number of active interfaces required for the port-channel interface to become active:

```
port-channel min-bundle number
```

Example:

```
ciscoasa(config-if)# port-channel min-bundle 2
```

The *number* is between 1 and 16. The default is 1. If the active interfaces in the channel group falls below this value, then the port-channel interface goes down, and could trigger a device-level failover.

**Step 4** Configure the load-balancing algorithm:

```
```

Example:

ciscoasa(config-if)# port-channel load-balance src-dst-mac

By default, the ASA balances the packet load on interfaces according to the source and destination IP address (src-dst-ip) of the packet. If you want to change the properties on which the packet is categorized, use this command. For example, if your traffic is biased heavily towards the same source and destination IP addresses, then the traffic assignment to interfaces in the EtherChannel will be unbalanced. Changing to a different algorithm can result in more evenly distributed traffic.

**Step 5**
Set the LACP system priority:

```
lacp system-priority number
```

Example:

ciscoasa(config)# lacp system-priority 12345

The *number* is between 1 and 65535. The default is 32768. The higher the number, the lower the priority. This command is global for the ASA.

If the device at the other end of the EtherChannel has conflicting port priorities, the system priority is used to determine which port priorities to use. For interface priorities within an EtherChannel, see the `lacp port-priority` command.

**Step 6**
(Optional) Set the Ethernet properties for the port-channel interface to override the properties set on the individual interfaces.

See [Enable the Physical Interface and Configure Ethernet Parameters](#) for Ethernet commands. This method provides a shortcut to set these parameters because these parameters must match for all interfaces in the channel group.

---

**Related Topics**

- [Load Balancing](#)
- [Add Interfaces to the EtherChannel](#)

---

**Configure VLAN Subinterfaces and 802.1Q Trunking**

Subinterfaces let you divide a physical, redundant, or EtherChannel interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or ASAs. This feature is particularly useful in multiple context mode so that you can assign unique interfaces to each context.

**Before You Begin**

- Preventing untagged packets on the physical interface—If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. This property is also true for the active physical interface in a redundant interface pair and for EtherChannel links. Because the physical, redundant, or EtherChannel interface must be enabled for the subinterface to pass traffic, ensure that the physical, redundant, or EtherChannel interface does not pass traffic by leaving out the `nameif` command. If you want to let the physical, redundant, or EtherChannel interface pass untagged packets, you can configure the `nameif` command as usual.
- (ASA 5555-X and lower) You cannot configure subinterfaces on the Management 0/0 interface.

The ASA does not support the Dynamic Trunking Protocol (DTP), so you must configure the connected switch port to trunk unconditionally.

For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.

### Procedure

#### Step 1
Specify the new subinterface:

```
interface {physical_interface | redundant number | port-channel number}.subinterface
```

Example:
```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

The `redundant number` argument is the redundant interface ID, such as `redundant 1`.

The `port-channel number` argument is the EtherChannel interface ID, such as `port-channel 1`.

The `subinterface` ID is an integer between 1 and 4294967293.

#### Step 2
Specify the VLAN for the subinterface:

```
vlan vlan_id
```

Example:
```
ciscoasa(config-subif)# vlan 101
```

The `vlan_id` is an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.

You can only assign a single VLAN to a subinterface, and you cannot assign the same VLAN to multiple subinterfaces. You cannot assign a VLAN to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the `no` option; you can enter the `vlan` command with a different VLAN ID, and the ASA changes the old ID.

### Related Topics
- Licensing for ASA Appliance Interfaces, page 9-10

## Enable Jumbo Frame Support

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 maximum use of other features, such as ACLs.

### Before You Begin
- In multiple context mode, set this option in the system execution space.
- Changes in this setting require you to reload the ASA.
• Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9198 using the `mtu` command. In multiple context mode, set the MTU within each context.

• Be sure to adjust the TCP MSS, either to disable it for non-VPN traffic (use the `sysopt connection tcpmss 0` command), or to increase it in accord with the MTU.

**Procedure**

**Step 1**
Enable jumbo frame support:

```
jumbo-frame reservation
```

**Examples**
The following example enables jumbo frame reservation, saves the configuration, and reloads the ASA:

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4ed04610 69af58d0 0a6b7cb5
70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

**Related Topics**
• Control Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size, page 9-7
• Configuring the MAC Address, MTU, and TCP MSS, page 11-9

**Monitoring Interfaces**

See the following commands:

• `show interface`
  Displays interface statistics.

• `show interface ip brief`
  Displays interface IP addresses and status.

• `show lacp [{channel_group_number} {counters | internal | neighbor | sys-id}]`
  For EtherChannel, displays LACP information such as traffic statistics, system identifier and neighbor details.

• `show port-channel [channel_group_number] [brief | detail | port | protocol | summary]`
  For EtherChannel, displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
Examples for ASA Appliance Interfaces

See the following configuration examples.

- Physical Interface Parameters Example, page 9-24
- Subinterface Parameters Example, page 9-24
- Multiple Context Mode Example, page 9-24
- EtherChannel Example, page 9-25

Physical Interface Parameters Example

The following example configures parameters for the physical interface in single mode:

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

Subinterface Parameters Example

The following example configures parameters for a subinterface in single mode:

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

Multiple Context Mode Example

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
interface gigabitethernet 0/1.1
    vlan 101
    context contextA
    allocate-interface gigabitethernet 0/1.1
```
EtherChannel Example

The following example configures three interfaces as part of an EtherChannel. It also sets the system priority to be a higher priority, and GigabitEthernet 0/2 to be a higher priority than the other interfaces in case more than eight interfaces are assigned to the EtherChannel.

lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip

History for ASA Appliance Interfaces

Table 9-2  History for ASA Appliance Interfaces

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased VLANs</td>
<td>7.0(5)</td>
<td>Increased the following limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ASA5510 Base license VLANs from 0 to 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ASA5510 Security Plus license VLANs from 10 to 25.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ASA5520 VLANs from 25 to 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ASA5540 VLANs from 100 to 200.</td>
</tr>
<tr>
<td>Increased interfaces for the</td>
<td>7.2(2)</td>
<td>For the Base license on the ASA 5510, the maximum number of interfaces was increased</td>
</tr>
<tr>
<td>Base license on the ASA 5510</td>
<td></td>
<td>from 3 plus a management interface to unlimited interfaces.</td>
</tr>
<tr>
<td>Increased VLANs</td>
<td>7.2(2)</td>
<td>VLAN limits were increased for the ASA 5510 (from 10 to 50 for the Base license, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA 5550 (from 200 to 250).</td>
</tr>
<tr>
<td>Gigabit Ethernet Support for</td>
<td>7.2(3)</td>
<td>The ASA 5510 ASA now supports GE (Gigabit Ethernet) for port 0 and 1 with the Security</td>
</tr>
<tr>
<td>the ASA 5510 Security Plus</td>
<td></td>
<td>Plus license. If you upgrade the license from Base to Security Plus, the capacity</td>
</tr>
<tr>
<td>License</td>
<td></td>
<td>of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ethernet 0/0 and Ethernet 0/1. Use the speed command to change the speed on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface and use the show interface command to see what speed is currently</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configured for each interface.</td>
</tr>
</tbody>
</table>
Table 9-2  History for ASA Appliance Interfaces (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant interfaces</td>
<td>8.0(2)</td>
<td>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.</td>
</tr>
<tr>
<td>Jumbo packet support for the ASA 5580</td>
<td>8.1(1)</td>
<td>The Cisco ASA 5580 supports jumbo frames. 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 maximum use of other features, such as ACLs. This feature is also supported on the ASA 5585-X. We introduced the following command: <code>jumbo-frame reservation</code></td>
</tr>
<tr>
<td>Increased VLANs for the ASA 5580</td>
<td>8.1(2)</td>
<td>The number of VLANs supported on the ASA 5580 are increased from 100 to 250.</td>
</tr>
<tr>
<td>Support for Pause Frames for Flow Control on the ASA 5580 Ten Gigabit Ethernet Interfaces</td>
<td>8.2(2)</td>
<td>You can now enable pause (XOFF) frames for flow control. This feature is also supported on the ASA 5585-X. We introduced the following command: <code>flowcontrol</code>.</td>
</tr>
<tr>
<td>Support for Pause Frames for Flow Control on Gigabit Ethernet Interfaces</td>
<td>8.2(5)/8.4(2)</td>
<td>You can now enable pause (XOFF) frames for flow control for Gigabit Ethernet interfaces on all models. We modified the following command: <code>flowcontrol</code>.</td>
</tr>
</tbody>
</table>
We introduced the following commands: `channel-group`, `lacp port-priority`, `interface port-channel`, `lacp max-bundle`, `port-channel min-bundle`, `port-channel load-balance`, `lacp system-priority`, `clear lacp counters`, `show lacp`, `show port-channel`.

Note: EtherChannel is not supported on the ASA 5505.

You can now configure up to 16 active links in an EtherChannel. Previously, you could have 8 active links and 8 standby links. Be sure that your switch can support 16 active links (for example the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module).

Note: If you upgrade from an earlier ASA version, the maximum active interfaces is set to 8 for compatibility purposes (the `lacp max-bundle` command).

We modified the following commands: `lacp max-bundle` and `port-channel min-bundle`.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EtherChannel support</td>
<td>8.4(1)</td>
<td>You can configure up to 48 802.3ad EtherChannels of eight active interfaces each. We introduced the following commands: <code>channel-group</code>, <code>lacp port-priority</code>, <code>interface port-channel</code>, <code>lacp max-bundle</code>, <code>port-channel min-bundle</code>, <code>port-channel load-balance</code>, <code>lacp system-priority</code>, <code>clear lacp counters</code>, <code>show lacp</code>, <code>show port-channel</code>. Note: EtherChannel is not supported on the ASA 5505.</td>
</tr>
<tr>
<td>Support for 16 active links in an EtherChannel</td>
<td>9.2(1)</td>
<td>You can now configure up to 16 active links in an EtherChannel. Previously, you could have 8 active links and 8 standby links. Be sure that your switch can support 16 active links (for example the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module). Note: If you upgrade from an earlier ASA version, the maximum active interfaces is set to 8 for compatibility purposes (the <code>lacp max-bundle</code> command). We modified the following commands: <code>lacp max-bundle</code> and <code>port-channel min-bundle</code>.</td>
</tr>
</tbody>
</table>
Basic Interface Configuration (ASAv)

This chapter includes tasks for starting your interface configuration for the Cisco ASAv, including configuring Ethernet settings, redundant interfaces, and VLAN subinterfaces.

- Information About Starting ASAv Interface Configuration, page 10-1
- Licensing Requirements for ASAv Interfaces, page 10-5
- Guidelines and Limitations, page 10-6
- Default Settings, page 10-7
- Starting Interface Configuration (ASAv), page 10-7
- Monitoring Interfaces, page 10-14
- Configuration Examples for ASAv Interfaces, page 10-14
- Where to Go Next, page 10-14
- Feature History for ASAv Interfaces, page 10-15

Information About Starting ASAv Interface Configuration

- ASAv Interfaces and Virtual NICs, page 10-1
- Interfaces in Transparent Mode, page 10-2
- Management Interface, page 10-2
- Redundant Interfaces, page 10-3
- Controlling Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size, page 10-3

ASAv Interfaces and Virtual NICs

As a guest on a virtualized platform, the ASAv utilizes the network interfaces of the underlying physical platform. Each ASAv interface maps to a virtual NIC (vNIC).

- ASAv Interfaces, page 10-2
- Supported vNICs, page 10-2
**ASA Interfaces**

The ASA includes the following Gigabit Ethernet interfaces:

- Management 0/0
- GigabitEthernet 0/0 through 0/8. Note that the GigabitEthernet 0/8 is used for the failover link when you deploy the ASA as part of a failover pair.

**Supported vNICs**

The ASA supports the following vNICs:

<table>
<thead>
<tr>
<th>vNIC Type</th>
<th>Hypervisor Support</th>
<th>ASA Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>e1000</td>
<td>VMware</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtio</td>
<td>No</td>
<td>KVM</td>
<td>9.3(2.200) and later</td>
</tr>
</tbody>
</table>

**Interfaces in Transparent Mode**

Interfaces in transparent mode belong to a “bridge group,” one bridge group for each network. You can have up to 8 bridge groups of 4 interfaces. For more information about bridge groups, see [Bridge Groups in Transparent Mode, page 12-1](#).

**Management Interface**

- [Management Interface Overview, page 10-2](#)
- [Using Any Interface for Management-Only Traffic, page 10-2](#)
- [Management Interface for Transparent Mode, page 10-3](#)
- [No Through Traffic Support, page 10-3](#)

**Management Interface Overview**

You can manage the ASA by connecting to:

- Any through-traffic interface
- The dedicated Management 0/0 interface

You may need to configure management access to the interface according to Chapter 35, “Management Access.”

**Using Any Interface for Management-Only Traffic**

You can use any interface as a dedicated management-only interface by configuring it for management traffic (see the `management-only` command).
Management Interface for Transparent Mode

In transparent firewall mode, in addition to the maximum allowed through-traffic interfaces, you can also use the Management 0/0 interface (either the physical interface or a subinterface) as a separate management interface. You cannot use any other interface types as management interfaces. The management interface is not part of a normal bridge group. Note that for operational purposes, it is part of a non-configurable bridge group.

Note

In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the ASA updates the MAC address table to use the management interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the ASA will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.

No Through Traffic Support

The Management 0/0 interface is always set to management-only; you cannot use this interface for through traffic support.

Redundant Interfaces

A logical redundant interface consists of a pair of physical interfaces: an active and a standby 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 device-level failover if desired.

Redundant Interface MAC Address

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see Configuring the MAC Address, MTU, and TCP MSS, page 11-9 or the Configure Multiple Contexts, page 6-14). When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Controlling Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size

- MTU Overview, page 10-4
- Default MTU, page 10-4
- Path MTU Discovery, page 10-4
- Setting the MTU and Jumbo Frames, page 10-4
MTU Overview

The maximum transmission unit (MTU) specifies the maximum frame payload size that the ASA can transmit on a given Ethernet interface. The MTU value is the frame size without Ethernet headers, FCS, or VLAN tagging. The Ethernet header is 14 bytes and the FCS is 4 bytes. When you set the MTU to 1500, the expected frame size is 1518 bytes including the headers. If you are using VLAN tagging (which adds an additional 4 bytes), then when you set the MTU to 1500, the expected frame size is 1522. Do not set the MTU value higher to accommodate these headers. For information about accommodating TCP headers for encapsulation, do not alter the MTU setting; instead change the TCP Maximum Segment Size (TCP Maximum Segment Size Overview, page 10-4).

Note

The ASA can receive frames larger than the configured MTU as long as there is room in memory. See Enabling Jumbo Frame Support, page 10-13 to increase memory for larger frames.

Default MTU

The default MTU on the ASA is 1500 bytes. This value does not include the 18 or more bytes for the Ethernet header, CRC, VLAN tagging, and so on.

Path MTU Discovery

The ASA supports Path MTU Discovery (as defined in RFC 1191), which lets all devices in a network path between two hosts coordinate the MTU so that they can standardize on the lowest MTU in the path.

Setting the MTU and Jumbo Frames

See Configuring the MAC Address, MTU, and TCP MSS, page 11-9.

See the following guidelines:

- Matching MTUs on the traffic path—We recommend that you set the MTU on all ASA interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.
- Accommodating jumbo frames—If you enable jumbo frames, you can set the MTU up to 9000 bytes.

TCP Maximum Segment Size Overview

The TCP maximum segment size (TCP MSS) is the size of the TCP payload before any TCP headers are added. UDP packets are not affected. The client and the server exchange TCP MSS values during the three-way handshake when establishing the connection.
You can set the TCP MSS on the ASA. If either endpoint of a connection requests a TCP MSS that is larger than the value set on the ASA, the ASA overwrites the TCP MSS in the request packet with the ASA maximum. If the host or server does not request a TCP MSS, then the ASA assumes the RFC 793-default value of 536 bytes, but does not modify the packet. You can also configure the minimum TCP MSS; if a host or server requests a very small TCP MSS, the ASA can adjust the value up. By default, the minimum TCP MSS is not enabled.

For example, you configure the default MTU of 1500 bytes. A host requests an MSS of 1700. If the ASA maximum TCP MSS is 1380, then the ASA changes the MSS value in the TCP request packet to 1380. The server then sends 1380-byte packets.

**Default TCP MSS**

By default, the maximum TCP MSS on the ASA is 1380 bytes. This default accommodates VPN connections where the headers can add up to 120 bytes; this value fits within the default MTU of 1500 bytes.

### Setting the TCP MSS for VPN and Non-VPN Traffic

See Configuring the MAC Address, MTU, and TCP MSS, page 11-9. See the following guidelines:

- **Non-VPN traffic**—If you do not use VPN and do not need extra space for headers, then you should disable the TCP MSS limit and accept the value established between connection endpoints. Because connection endpoints typically derive the TCP MSS from the MTU, non-VPN packets usually fit this TCP MSS.

- **VPN traffic**—Set the maximum TCP MSS to the MTU - 120. For example, if you use jumbo frames and set the MTU to a higher value, then you need to set the TCP MSS to accommodate the new MTU.

### Examples

The following example enables jumbo frames, increases the MTU on all interfaces, and disables the TCP MSS for non-VPN traffic (by setting the TCP MSS to 0, which means there is no limit):

```plaintext
jumbo frame-reservation
mtu inside 9000
mtu outside 9000
sysopt connection tcpmss 0
```

The following example enables jumbo frames, increases the MTU on all interfaces, and changes the TCP MSS for VPN traffic to 8880 (the MTU minus 120):

```plaintext
jumbo frame-reservation
mtu inside 9000
mtu outside 9000
sysopt connection tcpmss 8880
```
Guidelines and Limitations

For an interface to count against the VLAN limit, you must assign a VLAN to it. For example:

```
interface gigabitethernet 0/0.100
vlan 100
```

Interfaces of all types comprise the maximum number of combined interfaces; for example, VLANs, physical, redundant, and bridge group interfaces. Every `interface` command defined in the configuration counts against this limit.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Firewall Mode Guidelines

- For transparent mode, you can configure up to 8 bridge groups.
- Each bridge group can include up to 4 interfaces.

Failover Guidelines

- When you use a redundant interface as a failover link, it must be pre-configured on both units in the failover pair; you cannot configure it on the primary unit and expect it to replicate to the secondary unit because the failover link itself is required for replication.
- If you use a redundant interface for the state link, no special configuration is required; the configuration can replicate from the primary unit as normal.
- You can monitor redundant interfaces for failover using the `monitor-interface` command; be sure to reference the logical redundant interface name. When an active member interface fails over to a standby interface, this activity does not cause the redundant interface to appear to be failed when being monitored for device-level failover. Only when all physical interfaces fail does the redundant interface appear to be failed.
- You cannot share a failover or state interface with a data interface.

Redundant Interface Guidelines

- You can configure up to 8 redundant interface pairs.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAv5 and ASAv10</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Standard and Premium License: 50</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Standard and Premium License: 716</td>
</tr>
<tr>
<td>ASAv30</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Standard and Premium License: 200</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Standard and Premium License: 1316</td>
</tr>
</tbody>
</table>

Note
• All ASA configuration refers to the logical redundant interface instead of the member physical interfaces.
• If you shut down the active interface, then the standby interface becomes active.
• You cannot set a redundant interface as management-only.
• For failover guidelines, see Failover Guidelines, page 10-6.

Default Settings

This section lists default settings for interfaces if you do not have a factory default configuration. For information about the factory default configurations, see Factory Default Configurations, page 2-13.

Default State of Interfaces
• Physical interfaces—Disabled.
• Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
• Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Default Speed and Duplex
• By default, the speed and duplex for interfaces are set to auto-negotiate.

Default MAC Addresses
By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

Default vNIC
All interfaces use the E1000 emulation.

Starting Interface Configuration (ASAv)

• Task Flow for Starting Interface Configuration, page 10-7
• Enabling the Physical Interface and Configuring Ethernet Parameters, page 10-8
• Configuring a Redundant Interface, page 10-10
• Configuring VLAN Subinterfaces and 802.1Q Trunking, page 10-12
• Enabling Jumbo Frame Support, page 10-13

Task Flow for Starting Interface Configuration

To start configuring interfaces, perform the following steps:

Step 1  Enable the physical interface, and optionally change Ethernet parameters. See Enabling the Physical Interface and Configuring Ethernet Parameters, page 10-8.
Physical interfaces are disabled by default.
Step 2  (Optional) Configure redundant interface pairs. See Configuring a Redundant Interface, page 10-10.
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.

Step 3  (Optional) Configure VLAN subinterfaces. See Configuring VLAN Subinterfaces and 802.1Q Trunking, page 10-12.

Step 4  (Optional) Enable jumbo frame support according to Enabling Jumbo Frame Support, page 10-13.

Enabling the Physical Interface and Configuring Ethernet Parameters

This section describes how to:
- Enable the physical interface
- Set a specific speed and duplex
- Enable pause frames for flow control

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface physical_interface</code></td>
<td>Specifies the interface that you want to configure.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config)# interface gigabitethernet 0/0</code></td>
<td>Specifies the interface that you want to configure.</td>
</tr>
<tr>
<td></td>
<td>where the <code>physical_interface</code> ID includes the type, slot, and port</td>
</tr>
<tr>
<td></td>
<td>number as <code>type[slot]/port</code>.</td>
</tr>
<tr>
<td></td>
<td>The physical interface types include the following:</td>
</tr>
<tr>
<td></td>
<td>- <code>gigabitethernet</code></td>
</tr>
<tr>
<td></td>
<td>- <code>management</code></td>
</tr>
<tr>
<td></td>
<td>Enter the type followed by <code>slot/port</code>, for example, <code>gigabitethernet0/1</code>. A space is optional between the type and the slot/port.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Sets the speed. The default setting is <code>auto</code>.</td>
</tr>
<tr>
<td>`speed {auto</td>
<td>10</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config-if)# speed 100</code></td>
<td>Sets the speed. The default setting is <code>auto</code>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the duplex. The <code>auto</code> setting is the default.</td>
</tr>
<tr>
<td>`duplex {auto</td>
<td>full</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config-if)# duplex full</code></td>
<td>Sets the duplex. The <code>auto</code> setting is the default.</td>
</tr>
</tbody>
</table>
Step 4
(Optional)

**flowcontrol send on [low_water high_water pause_time] [noconfirm]**

**Example:**
ciscoasa(config-if)# flowcontrol send on 95 200 10000

Enables pause (XOFF) frames for flow control.

If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue. Pause (XOFF) and XON frames are generated automatically by the NIC hardware based on the FIFO buffer usage. A pause frame is sent when the buffer usage exceeds the high-water mark. The default high_water value is 24 KB; you can set it between 0 and 47 KB. After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark. By default, the low_water value is 16 KB; you can set it between 0 and 47 KB. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by the timer value in the pause frame. The default pause_time value is 26624; you can set it between 0 and 65535. If the buffer usage is consistently above the high-water mark, pause frames are sent repeatedly, controlled by the pause refresh threshold value.

When you use this command, you see the following warning:

Changing flow-control parameters will reset the interface. Packets may be lost during the reset. Proceed with flow-control changes?

To change the parameters without being prompted, use the noconfirm keyword.

**Note** Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Step 5

**no shutdown**

**Example:**
ciscoasa(config-if)# no shutdown

Enables the interface. To disable the interface, enter the shutdown command. If you enter the shutdown command, you also shut down all subinterfaces. If you shut down an interface in the system execution space, then that interface is shut down in all contexts that share it.

What to Do Next

Optional Tasks:
- Configure redundant interface pairs. See Configuring a Redundant Interface, page 10-10.
- Configure VLAN subinterfaces. See Configuring VLAN Subinterfaces and 802.1Q Trunking, page 10-12.

Required Tasks:
- Complete the interface configuration. See Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”
Configuring a Redundant Interface

A logical redundant interface consists of a pair of physical interfaces: an active and a standby 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.

This section describes how to configure redundant interfaces.

- Configuring a Redundant Interface, page 10-10
- Changing the Active Interface, page 10-11

Configuring a Redundant Interface

This section describes how to create a redundant interface. By default, redundant interfaces are enabled.

Guidelines and Limitations

- You can configure up to 8 redundant interface pairs.
- Redundant interface delay values are configurable, but by default the ASA inherits the default delay values based on the physical type of its member interfaces.
- See also Redundant Interface Guidelines, page 10-6.

Prerequisites

- Both member interfaces must be of the same physical type. For example, both must be GigabitEthernet.
- You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the no nameif command.

⚠️ Caution

If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 interface redundant number</td>
<td>Adds the logical redundant interface, where the number argument is an integer between 1 and 8.</td>
</tr>
<tr>
<td>Example: ciscoasa(config)# interface redundant 1</td>
<td>Note You need to add at least one member interface to the redundant interface before you can configure logical parameters for it such as a name.</td>
</tr>
</tbody>
</table>
Chapter 10      Basic Interface Configuration (ASAv)

Starting Interface Configuration (ASAv)

Examples

The following example creates two redundant interfaces:

```
ciscoasa(config)# interface redundant 1
(ciscoasa(config-if)# member-interface gigabitethernet 0/0
(ciscoasa(config-if)# member-interface gigabitethernet 0/1
(ciscoasa(config-if)# interface redundant 2
(ciscoasa(config-if)# member-interface gigabitethernet 0/2
(ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

What to Do Next

Optional Task:
- Configure VLAN subinterfaces. See Configuring VLAN Subinterfaces and 802.1Q Trunking, page 10-12.

Required Tasks:
- Complete the interface configuration. See Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”

Changing the Active Interface

By default, the active interface is the first interface listed in the configuration, if it is available. To view which interface is active, enter the following command:

```
ciscoasa# show interface redundantnumber detail | grep Member
```

For example:

```
ciscoasa# show interface redundant1 detail | grep Member
Members GigabitEthernet0/3 (Active), GigabitEthernet0/2
```

To change the active interface, enter the following command:

```
ciscoasa# redundant-interface redundantnumber active-member physical_interface
```

where the `redundantnumber` argument is the redundant interface ID, such as `redundant1`.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td><code>member-interface physical_interface</code></td>
<td>Adds the first member interface to the redundant interface. After you add the interface, any configuration for it (such as an IP address) is removed.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config-if)# member-interface gigabitethernet 0/0</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td><code>member-interface physical_interface</code></td>
<td>Adds the second member interface to the redundant interface. Make sure the second interface is the same physical type as the first interface. To remove a member interface, enter the no <code>member-interface physical_interface</code> command. You cannot remove both member interfaces from the redundant interface; the redundant interface requires at least one member interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config-if)# member-interface gigabitethernet 0/1</td>
<td></td>
</tr>
</tbody>
</table>
The physical_interface is the member interface ID that you want to be active.

Configuring VLAN Subinterfaces and 802.1Q Trunking

Subinterfaces let you divide a physical or redundant interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or ASAs.

Guidelines and Limitations

- Maximum subinterfaces—To determine how many VLAN subinterfaces are allowed for your model, see Licensing Requirements for ASAv Interfaces, page 10-5.

- Preventing untagged packets on the physical interface—If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. This property is also true for the active physical interface in a redundant interface pair. Because the physical or redundant interface must be enabled for the subinterface to pass traffic, ensure that the physical or redundant interface does not pass traffic by leaving out the nameif command. If you want to let the physical or redundant interface pass untagged packets, you can configure the nameif command as usual. See Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces,” for more information about completing the interface configuration.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>**interface (physical_interface</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies the new subinterface. See Enabling the Physical Interface and Configuring Ethernet Parameters, page 10-8 for a description of the physical interface ID.</td>
</tr>
<tr>
<td>ciscoasa(config)# interface</td>
<td>The redundant number argument is the redundant interface ID, such as <strong>redundant 1</strong>.</td>
</tr>
<tr>
<td>gigabitethernet 0/1.100</td>
<td>The subinterface ID is an integer between 1 and 4294967293.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>vlan vlan_id</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies the VLAN for the subinterface. The vlan_id is an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.</td>
</tr>
<tr>
<td>ciscoasa(config-subif)# vlan 101</td>
<td>You can only assign a single VLAN to a subinterface, and you cannot assign the same VLAN to multiple subinterfaces. You cannot assign a VLAN to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the no option; you can enter the vlan command with a different VLAN ID, and the ASA changes the old ID.</td>
</tr>
</tbody>
</table>
What to Do Next

Optional Task:

Required Tasks:
- Complete the interface configuration. See Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”

Enabling Jumbo Frame Support

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 maximum use of other features, such as ACLs. See Controlling Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size, page 10-3 for more information.

Prerequisites

- Changes in this setting require you to reload the ASA.
- Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9000 using the \texttt{mtu} command. See Configuring the MAC Address, MTU, and TCP MSS, page 11-9.
- Be sure to adjust the TCP MSS, either to disable it for non-VPN traffic (using the \texttt{sysopt connection tcpmss 0} command), or to increase it in accord with the MTU according to Configuring the MAC Address, MTU, and TCP MSS, page 11-9.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>jumbo-frame reservation</td>
<td>Enables jumbo frame support. To disable jumbo frames, use the \texttt{no} form of this command.</td>
</tr>
</tbody>
</table>

Example:
\[
\text{ciscoasa(config)# jumbo-frame reservation}
\]

Examples

The following example enables jumbo frame reservation, saves the configuration, and reloads the ASA:

\[
\text{ciscoasa(config)# jumbo-frame reservation}
\]

WARNING: this command will take effect after the running-config is saved and the system has been rebooted. Command accepted.

\[
\text{ciscoasa(config)# write memory}
\]

Building configuration...
Crypochecksum: 718e3706 4edb11ea 69af5880 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
\[
\text{ciscoasa(config)# reload}
\]

Proceed with reload? [confirm] \textbf{Y}


What to Do Next

Complete the interface configuration. See Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”

Monitoring Interfaces

To monitor interfaces, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface</td>
<td>Displays interface statistics.</td>
</tr>
<tr>
<td>show interface ip brief</td>
<td>Displays interface IP addresses and status.</td>
</tr>
</tbody>
</table>

Configuration Examples for ASAv Interfaces

- Physical Interface Parameters Example, page 10-14
- Subinterface Parameters Example, page 10-14

Physical Interface Parameters Example

The following example configures parameters for the physical interface:

```
interface gigabitethernet 0/1
  speed 1000
  duplex full
  no shutdown
```

Subinterface Parameters Example

The following example configures parameters for a subinterface:

```
interface gigabitethernet 0/1.1
  vlan 101
  no shutdown
```

Where to Go Next

Complete the interface configuration according to Chapter 11, “Routed Mode Interfaces,” or Chapter 12, “Transparent Mode Interfaces.”
## Feature History for ASAv Interfaces

### Table 10-1  Feature History for Interfaces

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAv support</td>
<td>9.2(1)</td>
<td>The ASAv was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 11

Routed Mode Interfaces

This chapter includes tasks to complete the interface configuration for all models in routed firewall mode.

- Information About Completing Interface Configuration in Routed Mode, page 11-1
- Licensing Requirements for Completing Interface Configuration in Routed Mode, page 11-2
- Guidelines and Limitations, page 11-4
- Default Settings, page 11-5
- Completing Interface Configuration in Routed Mode, page 11-5
- Turning Off and Turning On Interfaces, page 11-16
- Monitoring Interfaces, page 11-16
- Feature History for Interfaces in Routed Mode, page 11-17

Note

For multiple context mode, complete the tasks in this section in the context execution space. Enter the `changeto context name` command to change to the context you want to configure.

Information About Completing Interface Configuration in Routed Mode

- Security Levels, page 11-1
- Dual IP Stack (IPv4 and IPv6), page 11-2

Security Levels

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See Allowing Same Security Level Communication, page 11-14 for more information.

The level controls the following behavior:
Licensing Requirements for Completing Interface Configuration in Routed Mode

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an ACL to the interface.

If you enable communication for same security interfaces (see Allowing Same Security Level Communication, page 11-14), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the ASA.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

If you enable communication for same security interfaces, you can filter traffic in either direction.

- established command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

If you enable communication for same security interfaces, you can configure established commands for both directions.

Dual IP Stack (IPv4 and IPv6)

The Cisco ASA supports the configuration of both IPv6 and IPv4 on an interface. You do not need to enter any special commands to do so; simply enter the IPv4 configuration commands and IPv6 configuration commands as you normally would. Make sure you configure a default route for both IPv4 and IPv6.

Licensing Requirements for Completing Interface Configuration in Routed Mode
<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 5</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 30</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 536</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 636</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 50</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 716</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 916</td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 916</td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 200</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1316</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 300</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1716</td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 500</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 2516</td>
</tr>
<tr>
<td>ASA 5585-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base and Security Plus License: 1024</td>
</tr>
<tr>
<td></td>
<td>Interface Speed for SSP-10 and SSP-20:</td>
</tr>
<tr>
<td></td>
<td>Base License—1-Gigabit Ethernet for fiber interfaces</td>
</tr>
<tr>
<td></td>
<td>10 GE I/O License (Security Plus)—10-Gigabit Ethernet for fiber interfaces</td>
</tr>
<tr>
<td></td>
<td>(SSP-40 and SSP-60 support 10-Gigabit Ethernet by default.)</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base and Security Plus License: 4612</td>
</tr>
</tbody>
</table>
Note

For an interface to count against the VLAN limit, you must assign a VLAN to it. For example:

```
interface gigabitethernet 0/0.100
vlan 100
```

Interfaces of all types comprise the maximum number of combined interfaces; for example, VLANs, physical, redundant, bridge group, and EtherChannel interfaces. Every `interface` command defined in the configuration counts against this limit. For example, both of the following interfaces count even if the GigabitEthernet 0/0 interface is defined as part of port-channel 1:

```
interface gigabitethernet 0/0
```

and

```
interface port-channel 1
```

---

### Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

#### Context Mode Guidelines

- For the ASA 5512-X and higher in multiple context mode, configure the physical interfaces in the system execution space according to Chapter 9, “Basic Interface Configuration (ASA Appliances).” Then, configure the logical interface parameters in the context execution space according to this chapter. For the ASASM in multiple context mode, configure switch ports and VLANs on the switch, and then assign VLANs to the ASASM according to the ASASM quick start guide.

  The ASAv does not support multiple context mode.

- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.

- PPPoE is not supported in multiple context mode.

#### Firewall Mode Guidelines

Supported in routed firewall mode. For transparent mode, see Chapter 12, “Transparent Mode Interfaces.”

#### Failover Guidelines

Do not finish configuring failover interfaces with the procedures in this chapter. See Chapter 7, “Failover for High Availability,” to configure the failover and state links. In multiple context mode, failover interfaces are configured in the system configuration.

#### IPv6 Guidelines

Supports IPv6.
**VLAN ID Guidelines for the ASASM**

You can add any VLAN ID to the configuration, but only VLANs that are assigned to the ASA by the switch can pass traffic. To view all VLANs assigned to the ASA, use the `show vlan` command.

If you add an interface for a VLAN that is not yet assigned to the ASA by the switch, the interface will be in the down state. When you assign the VLAN to the ASA, the interface changes to an up state. See the `show interface` command for more information about interface states.

**Default Settings**

This section lists default settings for interfaces if you do not have a factory default configuration. For information about the factory default configurations, see Factory Default Configurations, page 2-13.

**Default Security Level**

The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly, then the ASA sets the security level to 100.

**Note**

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the `clear local-host` command.

**Default State of Interfaces for the ASASM**

- In single mode or in the system execution space, VLAN interfaces are enabled by default.
- In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

**Jumbo Frame Support**

By default, the ASASM supports jumbo frames. Just configure the MTU for the desired packet size according to Configuring the MAC Address, MTU, and TCP MSS, page 11-9.

**Completing Interface Configuration in Routed Mode**

- Task Flow for Completing Interface Configuration, page 11-5
- Configuring General Interface Parameters, page 11-6
- Configuring the MAC Address, MTU, and TCP MSS, page 11-9
- Configuring IPv6 Addressing, page 11-11
- Allowing Same Security Level Communication, page 11-14

**Task Flow for Completing Interface Configuration**

**Step 1**

Set up your interfaces depending on your model:
Completing Interface Configuration in Routed Mode

- ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
- ASASM—ASASM quick start guide.
- ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”

Step 2 (Multiple context mode) Allocate interfaces to the context according to Configure Multiple Contexts, page 6-14.

Step 3 (Multiple context mode) Enter the `change to context name` command to change to the context you want to configure. Configure general interface parameters, including the interface name, security level, and IPv4 address. See Configuring General Interface Parameters, page 11-6.

Step 4 (Optional) Configure the MAC address and the MTU. See Configuring the MAC Address, MTU, and TCP MSS, page 11-9.


Step 6 (Optional) Allow same security level communication, either by allowing communication between two interfaces or by allowing traffic to enter and exit the same interface. See Allowing Same Security Level Communication, page 11-14.

Configuring General Interface Parameters

This procedure describes how to set the name, security level, IPv4 address and other options.

For the ASA 5512-X and higher and the ASAv, you must configure interface parameters for the following interface types:
- Physical interfaces
- VLAN subinterfaces
- Redundant interfaces
- EtherChannel interfaces

For the ASASM, you must configure interface parameters for the following interface types:
- VLAN interfaces

Guidelines and Limitations

If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See Chapter 7, “Failover for High Availability,” to configure the failover and state links.

Restrictions

- PPPoE is not supported in multiple context mode.
- PPPoE and DHCP are not supported on the ASASM.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide
In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.

In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the `changeto context name` command.

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| For the ASA 5512-X and higher and ASAv:  
`interface {{(redundant number | port-channel number | physical_interface)}.{subinterface} | mapped_name}}`  

For the ASASM:  
ciscoasa(config)# interface {vlan number | mapped_name}  

**Example:**  
ciscoasa(config)# interface gigabithernet 0/0  

If you are not already in interface configuration mode, enters interface configuration mode.  
The `redundant number` argument is the redundant interface ID, such as `redundant 1`.  
The `port-channel number` argument is the EtherChannel interface ID, such as `port-channel 1`.  
See Enable the Physical Interface and Configure Ethernet Parameters, page 9-14 section for a description of the physical interface ID.  
Append the `subinterface` ID to the physical or redundant interface ID separated by a period (.)  
In multiple context mode, enter the `mapped_name` if one was assigned using the `allocate-interface` command. |
| **Step 2** | nameif name  

**Example:**  
ciscoasa(config-if)# nameif inside  

Names the interface.  
The `name` is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the `no` form, because that command causes all commands that refer to that name to be deleted. |
| **Step 3** | Do one of the following:  

**ip address** ip_address [mask] [standby ip_address]  

**Example:**  
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2  

Sets the IP address manually.  
**Note** For use with failover, you must set the IP address and standby address manually; DHCP and PPPoE are not supported.  
The `ip_address` and `mask` arguments set the interface IP address and subnet mask.  
The `standby ip_address` argument is used for failover. See Configure Active/Standby Failover, page 7-25 or the Configure Active/Active Failover, page 7-29 for more information. |
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip address dhcp [setroute]</code></td>
<td>Obtains an IP address from a DHCP server. The <code>setroute</code> keyword lets the ASA use the default route supplied by the DHCP server. Reenter this command to reset the DHCP lease and request a new lease. If you do not enable the interface using the <code>no shutdown</code> command before you enter the <code>ip address dhcp</code> command, some DHCP requests might not be sent.</td>
</tr>
</tbody>
</table>

Example:

ciscoasa(config-if)# ip address dhcp

To obtain an IP address from a PPPoE server, see the VPN configuration guide. PPPoE is not supported in multiple context mode.

---

### Step 4

**security-level number**

Sets the security level, where `number` is an integer between 0 (lowest) and 100 (highest). See Security Levels, page 11-1.

Example:

ciscoasa(config-if)# security-level 50

---

### Step 5

(Optional)

**management-only**

Sets an interface to management-only mode so that it does not pass through traffic.

Example:

ciscoasa(config-if)# management-only

By default, Management interfaces are configured as management-only. To disable this setting, enter the `no management-only` command.

(ASA 5512-X through ASA 5555-X) You cannot disable `management-only` on the Management 0/0 interface.

The `management-only` command is not supported for a redundant interface.

---

### Example

The following example configures parameters for VLAN 101:

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
```

```
ciscoasa(config-if)# security-level 100
```

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

The following example configures parameters in multiple context mode for the context configuration. The interface ID is a mapped name.

```
ciscoasa/contextA(config)# interface int1
```

```
ciscoasa/contextA(config-if)# nameif outside
```

```
ciscoasa/contextA(config-if)# security-level 100
```

```
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

### What to Do Next

- (Optional) Configure the MAC address and the MTU. See Configuring the MAC Address, MTU, and TCP MSS, page 11-9.
Configuring the MAC Address, MTU, and TCP MSS

This section describes how to configure MAC addresses for interfaces, how to set the MTU, and set the TCP MSS.

Information About MAC Addresses

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

For the ASASM, all VLANs use the same MAC address provided by the backplane.

A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this command, then it is used regardless of the member interface MAC addresses.

For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses the lowest numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can manually configure a MAC address for the port-channel interface. In multiple context mode, you can automatically assign unique MAC addresses to interfaces, including an EtherChannel port interface. We recommend manually, or in multiple context mode, automatically configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the ASA easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See How the ASA Classifies Packets, page 6-3 for more information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See Assign MAC Addresses to Context Interfaces Automatically, page 6-23 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use this procedure to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

Information About the MTU and TCP MSS

See Control Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size, page 9-7.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
• In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the `changeto context name` command.

• To increase the MTU above 1500, enable jumbo frames according to Enable Jumbo Frame Support, page 9-22. Jumbo frames are supported by default on the ASASM; you do not need to enable them.

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you are not already in interface configuration mode, enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>For the ASA 5512-X and higher and the ASAv:</strong>&lt;br&gt;`interface {{redundant number</td>
<td>port-channel number</td>
</tr>
<tr>
<td><strong>For the ASASM:</strong>&lt;br&gt;`ciscoasa(config)# interface {vlan number</td>
<td>mapped_name}`</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa(config)# interface vlan 100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Assigns a private MAC address to this interface. The <code>mac_address</code> is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE. The first two bytes of a manual MAC address cannot be A2 if you also want to use auto-generated MAC addresses. For use with failover, set the <code>standby</code> MAC address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.</td>
</tr>
<tr>
<td><code>mac-address mac_address</code>&lt;br&gt; <code>[standby mac_address]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa(config-if)# mac-address 000C.F142.4CDE</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the MTU between 300 and 9198 bytes (9000 for the ASAv). The default is 1500 bytes. For models that support jumbo frames, if you enter a value for any interface that is greater than 1500, then you need to enable jumbo frame support. See Enable Jumbo Frame Support, page 9-22.</td>
</tr>
<tr>
<td><code>mtu interface_name bytes</code></td>
<td><strong>Note</strong> When you set the MTU for a redundant or port-channel interface, the ASA applies the setting to all member interfaces. For the <code>minimum</code> keyword, sets the maximum segment size to be no less than <code>bytes</code>, between 48 and 65535. The minimum feature is disabled by default (set to 0).</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa(config)# mtu inside 9200</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting bytes to 0.</td>
</tr>
<tr>
<td><code>sysopt connection tcpmss [minimum] bytes</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa(config)# sysopt connection tcpmss 8500</code>&lt;br&gt;<code>ciscoasa(config)# sysopt connection tcpmss minimum 1290</code></td>
<td></td>
</tr>
</tbody>
</table>
Completing Interface Configuration in Routed Mode

What to Do Next


Configuring IPv6 Addressing

This section describes how to configure IPv6 addressing.

- Information About IPv6, page 11-11
- Configuring a Global IPv6 Address, page 11-12
- Configuring IPv6 Neighbor Discovery, page 11-13

Information About IPv6

This section includes information about how to configure IPv6.

- IPv6 Addressing, page 11-11
- Modified EUI-64 Interface IDs, page 11-11

IPv6 Addressing

You can configure two types of unicast addresses for IPv6:

- Global—The global address is a public address that you can use on the public network.
- Link-local—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the ND functions such as address resolution and neighbor discovery.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

Note

If you want to only configure the link-local addresses, see the `ipv6 enable` (to auto-configure) or `ipv6 address link-local` (to manually configure) command in the command reference.

Modified EUI-64 Interface IDs

RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture requires that the interface identifier portion of all unicast IPv6 addresses, except those that start with binary value 000, be 64 bits long and be constructed in Modified EUI-64 format. The ASA can enforce this requirement for hosts attached to the local link.

When this feature is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the IPv6 packets do not use the Modified EUI-64 format for the interface identifier, the packets are dropped and the following system log message is generated:

`%ASA-3-325003: EUI-64 source address check failed.`
Completing Interface Configuration in Routed Mode

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

Configuring a Global IPv6 Address

To configure a global IPv6 address, perform the following steps.

Note
Configuring the global address automatically configures the link-local address, so you do not need to configure it separately.

Restrictions

The ASA does not support IPv6 anycast addresses.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the changeto context name command.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** For the ASA 5512-X and higher and the ASAv:  
  `interface {redundant number | port-channel number | physical_interface}{.subinterface | mapped_name}`  
  For the ASASM:  
  `ciscoasa(config)# interface {vlan number | mapped_name}`  
  **Example:**  
  `ciscoasa(config)# interface gigabitethernet 0/0` | If you are not already in interface configuration mode, enters interface configuration mode.  
  The redundant number argument is the redundant interface ID, such as `redundant 1`.  
  The port-channel number argument is the EtherChannel interface ID, such as `port-channel 1`.  
  See Enable the Physical Interface and Configure Ethernet Parameters, page 9-14 for a description of the physical interface ID.  
  Append the subinterface ID to the physical or redundant interface ID separated by a period (.).  
  In multiple context mode, enter the mapped_name if one was assigned using the allocate-interface command. |

| Step 2 Do one of the following: | |
### Command | Purpose
---|---
`ipv6 address autoconfig` | Enables stateless autoconfiguration on the interface. Enabling stateless autoconfiguration on the interface configures IPv6 addresses based on prefixes received in Router Advertisement messages. A link-local address, based on the Modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled.

**Note** Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the ASA does send Router Advertisement messages in this case. See the `ipv6 nd suppress-ra` command to suppress messages.

`ipv6 address ipv6-address/prefix-length [standby ipv6-address]` | Assigns a global address to the interface. When you assign a global address, the link-local address is automatically created for the interface.

`standby` specifies the interface address used by the secondary unit or failover group in a failover pair.

`ipv6 address ipv6-prefix/prefix-length eui-64` | Assigns a global address to the interface by combining the specified prefix with an interface ID generated from the interface MAC address using the Modified EUI-64 format. When you assign a global address, the link-local address is automatically created for the interface.

You do not need to specify the standby address; the interface ID will be generated automatically.

**Step 3** *(Optional)*

`ipv6 enforce-eui64 if_name` | Enforces the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link.

The `if_name` argument is the name of the interface, as specified by the `nameif` command, on which you are enabling the address format enforcement.

See *Modified EUI-64 Interface IDs, page 11-11* for more information.

### Configuring IPv6 Neighbor Discovery

Allowing Same Security Level Communication

By default, interfaces on the same security level cannot communicate with each other, and packets cannot enter and exit the same interface. This section describes how to enable inter-interface communication when interfaces are on the same security level, and how to enable intra-interface communication.

Information About Inter-Interface Communication

Allowing interfaces on the same security level to communicate with each other provides the following benefits:

- You can configure more than 101 communicating interfaces.
  
  If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).

- You want traffic to flow freely between all same security interfaces without ACLs.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

Information About Intra-Interface Communication

Intra-interface communication might be useful for VPN traffic that enters an interface, but is then routed out the same interface. The VPN traffic might be unencrypted in this case, or it might be reencrypted for another VPN connection. For example, if you have a hub and spoke VPN network, where the ASA is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the ASA and then out again to the other spoke.

Note

All traffic allowed by this feature is still subject to firewall rules. Be careful not to create an asymmetric routing situation that can cause return traffic not to traverse the ASA.

For the ASASM, before you can enable this feature, you must first correctly configure the MSFC so that packets are sent to the ASA MAC address instead of being sent directly through the switch to the destination host. Figure 11-1 shows a network where hosts on the same interface need to communicate.
The following sample configuration shows the Cisco IOS `route-map` commands used to enable policy routing in the network shown in Figure 11-1:

```plaintext
route-map intra-inter3 permit 0
  match ip address 103
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
  match ip address 102
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
  match ip address 101
  set interface Vlan20
  set ip next-hop 10.6.34.7
```

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>same-security-traffic permit</code></td>
<td>Enables interfaces on the same security level so that they can communicate with each other.</td>
</tr>
<tr>
<td><code>inter-interface</code></td>
<td></td>
</tr>
<tr>
<td><code>same-security-traffic permit</code></td>
<td>Enables communication between hosts connected to the same interface.</td>
</tr>
<tr>
<td><code>intra-interface</code></td>
<td></td>
</tr>
</tbody>
</table>
Turning Off and Turning On Interfaces

This section describes how to turn off and on an interface.

All interfaces are enabled by default. In multiple context mode, if you disable or reenable the interface within a context, only that context interface is affected. But if you disable or reenable the interface in the system execution space, then you affect that interface for all contexts.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you are not already in interface configuration mode, enters interface configuration mode. In multiple context mode, enter the mapped_name if one was assigned using the allocate-interface command.</td>
</tr>
<tr>
<td>ciscoasa(config)# interface (vlan number</td>
<td>mapped_name)</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config)# interface vlan 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Disables the interface.</td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config-if)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Reenables the interface.</td>
</tr>
<tr>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config-if)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring Interfaces

To monitor interfaces, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface</td>
<td>Displays interface statistics.</td>
</tr>
<tr>
<td>show interface ip brief</td>
<td>Displays interface IP addresses and status.</td>
</tr>
</tbody>
</table>
Feature History for Interfaces in Routed Mode

Table 11-1 lists the release history for this feature.

Table 11-1  Feature History for Interfaces

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Increased VLANs                                  | 7.0(5)  | Increased the following limits:
|                                                  |          | • ASA5510 Base license VLANs from 0 to 10.                                            |
|                                                  |          | • ASA5510 Security Plus license VLANs from 10 to 25.                                  |
|                                                  |          | • ASA5520 VLANs from 25 to 100.                                                      |
|                                                  |          | • ASA5540 VLANs from 100 to 200.                                                    |
| Increased VLANs                                  | 7.2(2)  | The maximum number of VLANs for the Security Plus license on the ASA 5505 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 backup interface command is still useful for an Easy VPN configuration. VLAN limits were also increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), the ASA 5550 (from 200 to 250). |
| Gigabit Ethernet Support for the ASA 5510 Security Plus License | 7.2(3)  | The ASA 5510 now supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports 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 speed command to change the speed on the interface and use the show interface command to see what speed is currently configured for each interface. |
| Native VLAN support for the ASA 5505              | 7.2(4)/8.0(4) | You can now include the native VLAN in an ASA 5505 trunk port.                        |
|                                                  |          | We introduced the following command: switchport trunk native vlan.                   |
### Jumbo packet support for the ASA 5580
8.1(1)
The Cisco ASA 5580 supports jumbo frames. 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 maximum use of other features, such as ACLs.

We introduced the following command: `jumbo-frame reservation`.

### Increased VLANs for the ASA 5580
8.1(2)
The number of VLANs supported on the ASA 5580 are increased from 100 to 250.

### IPv6 support for transparent mode
8.2(1)
IPv6 support was introduced for transparent firewall mode.

### Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces
8.2(2)
You can now enable pause (XOFF) frames for flow control. We introduced the following command: `flowcontrol`.

#### Table 11-1  Feature History for Interfaces (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jumbo packet support for the ASA 5580</td>
<td>8.1(1)</td>
<td>The Cisco ASA 5580 supports jumbo frames. 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 maximum use of other features, such as ACLs. We introduced the following command: <code>jumbo-frame reservation</code>.</td>
</tr>
<tr>
<td>Increased VLANs for the ASA 5580</td>
<td>8.1(2)</td>
<td>The number of VLANs supported on the ASA 5580 are increased from 100 to 250.</td>
</tr>
<tr>
<td>IPv6 support for transparent mode</td>
<td>8.2(1)</td>
<td>IPv6 support was introduced for transparent firewall mode.</td>
</tr>
<tr>
<td>Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces</td>
<td>8.2(2)</td>
<td>You can now enable pause (XOFF) frames for flow control. We introduced the following command: <code>flowcontrol</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 12

Transparent Mode Interfaces

This chapter includes tasks to complete the interface configuration for all models in transparent firewall mode.

- Information About Transparent Mode Interfaces, page 12-1
- Licensing Requirements for Transparent Mode Interfaces, page 12-2
- Guidelines and Limitations for Transparent Mode Interfaces, page 12-4
- Default Settings for Transparent Mode Interfaces, page 12-5
- Completing Interface Configuration in Transparent Mode, page 12-6
- Turning Off and Turning On Interfaces, page 12-17
- Monitoring Interfaces, page 12-17
- Configuration Examples for Transparent Mode Interfaces, page 12-18
- Feature History for Transparent Mode Interfaces, page 12-19

Note

For multiple context mode, complete the tasks in this section in the context execution space. Enter the `changeto context name` command to change to the context you want to configure.

Information About Transparent Mode Interfaces

- Bridge Groups in Transparent Mode, page 12-1
- Security Levels, page 12-2

Bridge Groups in Transparent Mode

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; traffic is not routed to another bridge group within the Cisco ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context. At least one bridge group is required per context or in single mode.
Each bridge group requires a management IP address. For another method of management, see Management Interface, page 9-2.

Note

The ASA does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

Security Levels

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See Allowing Same Security Level Communication, page 12-16 for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an ACL to the interface.

  If you enable communication for same security interfaces (see Allowing Same Security Level Communication, page 12-16), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
  
  - NetBIOS inspection engine—Applied only for outbound connections.
  
  - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the ASA.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

  If you enable communication for same security interfaces, you can filter traffic in either direction.

- established command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host. If you enable communication for same security interfaces, you can configure established commands for both directions.

Licensing Requirements for Transparent Mode Interfaces
## Model License Requirement

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 5</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 30</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 536</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 636</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 50</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 716</td>
</tr>
<tr>
<td></td>
<td>Security Plus License: 916</td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 100</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 916</td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 200</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1316</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 300</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 1716</td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base License: 500</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base License: 2516</td>
</tr>
<tr>
<td>ASA 5585-X</td>
<td>VLANs:</td>
</tr>
<tr>
<td></td>
<td>Base and Security Plus License: 1024</td>
</tr>
<tr>
<td></td>
<td>Interface Speed for SSP-10 and SSP-20:</td>
</tr>
<tr>
<td></td>
<td>Base License—1-Gigabit Ethernet for fiber interfaces</td>
</tr>
<tr>
<td></td>
<td>10 GE I/O License (Security Plus)—10-Gigabit Ethernet for fiber interfaces</td>
</tr>
<tr>
<td></td>
<td>(SSP-40 and SSP-60 support 10-Gigabit Ethernet by default.)</td>
</tr>
<tr>
<td></td>
<td>Interfaces of all types:</td>
</tr>
<tr>
<td></td>
<td>Base and Security Plus License: 4612</td>
</tr>
</tbody>
</table>
For an interface to count against the VLAN limit, you must assign a VLAN to it. For example:

```
interface gigabitethernet 0/0.100
  vlan 100
```

Interfaces of all types comprise the maximum number of combined interfaces; for example, VLANs, physical, redundant, bridge group, and EtherChannel interfaces. Every `interface` command defined in the configuration counts against this limit. For example, both of the following interfaces count even if the GigabitEthernet 0/0 interface is defined as part of port-channel 1:

```
interface gigabitethernet 0/0
and
interface port-channel 1
```

### Guidelines and Limitations for Transparent Mode Interfaces

This section includes the guidelines and limitations for this feature.

**Context Mode Guidelines**

- For the ASA 5512-X and higher in multiple context mode, configure the physical interfaces in the system execution space according to [Chapter 9, “Basic Interface Configuration (ASA Appliances)”](#).
  Then, configure the logical interface parameters in the context execution space according to this chapter. For the ASASM in multiple context mode, configure switch ports and VLANs on the switch, and then assign VLANs to the ASASM according to the ASASM quick start guide.

The ASAv does not support multiple context mode.

- You can only configure context interfaces that you already assigned to the context in the system configuration using the `allocate-interface` command.

**Firewall Mode Guidelines**

- You can configure up to 250 bridge groups in single mode or per context in multiple mode. Note that you must use at least 1 bridge group; data interfaces must belong to a bridge group.
- Each bridge group can include up to 4 interfaces.
- For IPv4, a management IP address is required for each bridge group for both management traffic and for traffic to pass through the ASA.

Unlike routed mode, which requires an IP address for each interface, a transparent firewall has an IP address assigned to the entire bridge group. The ASA uses this IP address as the source address for packets originating on the ASA, such as system messages or AAA communications. In addition to the bridge group management address, you can optionally configure a management interface for some models; see [Management Interface, page 9-2](#) for more information.
The management IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255). The ASA does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported. See Configuring Bridge Groups, page 12-7 for more information about management IP subnets.

- For IPv6, at a minimum you need to configure link-local addresses for each interface for through traffic. For full functionality, including the ability to manage the ASA, you need to configure a global IPv6 address for each bridge group.
- For multiple context mode, each context must use different interfaces; you cannot share an interface across contexts.
- For multiple context mode, each context typically uses a different subnet. You can use overlapping subnets, but your network topology requires router and NAT configuration to make it possible from a routing standpoint.

### Failover Guidelines

Do not finish configuring failover interfaces with the procedures in this chapter. See Chapter 7, “Failover for High Availability,” to configure the failover and state links. In multiple context mode, failover interfaces are configured in the system configuration.

### IPv6 Guidelines

No support for IPv6 anycast addresses in transparent mode.

### VLAN ID Guidelines for the ASASM

You can add any VLAN ID to the configuration, but only VLANs that are assigned to the ASA by the switch can pass traffic. To view all VLANs assigned to the ASA, use the `show vlan` command.

If you add an interface for a VLAN that is not yet assigned to the ASA by the switch, the interface will be in the down state. When you assign the VLAN to the ASA, the interface changes to an up state. See the `show interface` command for more information about interface states.

## Default Settings for Transparent Mode Interfaces

This section lists default settings for interfaces if you do not have a factory default configuration. For information about the factory default configurations, see Factory Default Configurations, page 2-13.

### Default Security Level

The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly, then the ASA sets the security level to 100.

**Note**

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the `clear local-host` command.

### Default State of Interfaces for the ASASM

- In single mode or in the system execution space, VLAN interfaces are enabled by default.
In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

Jumbo Frame Support

By default, the ASASM supports jumbo frames. Just configure the MTU for the desired packet size according to Configuring the MAC Address, MTU, and TCP MSS, page 12-11.

Completing Interface Configuration in Transparent Mode

- Task Flow for Completing Interface Configuration, page 12-6
- Configuring Bridge Groups, page 12-7
- Configuring General Interface Parameters, page 12-8
- Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10
- Configuring the MAC Address, MTU, and TCP MSS, page 12-11
- Configuring IPv6 Addressing, page 12-14
- Allowing Same Security Level Communication, page 12-16

Task Flow for Completing Interface Configuration

**Step 1** Set up your interfaces depending on your model:
- ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
- ASASM—ASASM quick start guide.
- ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”

**Step 2** (Multiple context mode) Allocate interfaces to the context according to Configure Multiple Contexts, page 6-14.

**Step 3** (Multiple context mode) Enter the `changeto context name` command to change to the context you want to configure.

**Step 4** Configure one or more bridge groups, including the IPv4 address. See Configuring Bridge Groups, page 12-7.

**Step 5** Configure general interface parameters, including the bridge group it belongs to, the interface name, and security level. See Configuring General Interface Parameters, page 12-8.

**Step 6** (Optional) Configure a management interface. See Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10.

**Step 7** (Optional) Configure the MAC address and the MTU. See Configuring the MAC Address, MTU, and TCP MSS, page 12-11.

Step 9  (Optional) Allow same security level communication, either by allowing communication between two interfaces or by allowing traffic to enter and exit the same interface. See Allowing Same Security Level Communication, page 12-16.

Configuring Bridge Groups

Each bridge group requires a management IP address. The ASA uses this IP address as the source address for packets originating from the bridge group. The management IP address must be on the same subnet as the connected network. For IPv4 traffic, the management IP address is required to pass any traffic. For IPv6 traffic, you must, at a minimum, configure the link-local addresses to pass traffic, but a global management address is recommended for full functionality, including remote management and other management operations.

Guidelines and Limitations

You can configure up to 250 bridge groups in single mode or per context in multiple mode. Note that you must use at least one bridge group; data interfaces must belong to a bridge group.

Note  For a separate management interface (for supported models), a non-configurable bridge group (ID 301) is automatically added to your configuration. This bridge group is not included in the bridge group limit.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>interface bvi bridge_group_number</code></td>
<td>Creates a bridge group, where <code>bridge_group_number</code> is an integer between 1 and 250.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>ciscoasa(config)# interface bvi 1</code></td>
<td>Specifies the management IP address for the bridge group. Do not assign a host address (/32 or 255.255.255.255) to the bridge group. Also, do not use other subnets that contain fewer than 3 host addresses (one each for the upstream router, downstream router, and transparent firewall) such as a /30 subnet (255.255.255.252). The ASA drops all ARP packets to or from the first and last addresses in a subnet. Therefore, if you use a /30 subnet and assign a reserved address from that subnet to the upstream router, then the ASA drops the ARP request from the downstream router to the upstream router. The ASA does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported. The <code>standby</code> keyword and address is used for failover.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>ip address ip_address [mask] [standby ip_address]</code></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 12   Transparent Mode Interfaces

Completing Interface Configuration in Transparent Mode

Examples

The following example sets the management address and standby address of bridge group 1:

ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

What to Do Next


Configuring General Interface Parameters

This procedure describes how to set the name, security level, and bridge group for each transparent interface.

To configure a separate management interface, see Configuring a Management Interface (ASA 5512-X and Higher and ASAv), page 12-10.

For the ASA 5512-X and higher and the ASAv, you must configure interface parameters for the following interface types:

- Physical interfaces
- VLAN subinterfaces
- Redundant interfaces
- EtherChannel interfaces

For the ASASM, you must configure interface parameters for the following interface types:

- VLAN interfaces

Guidelines and Limitations

- You can configure up to four interfaces per bridge group.
- For information about security levels, see Security Levels, page 12-2.
- If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See Chapter 7, “Failover for High Availability,” to configure the failover and state links.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the changeto context name command.
## Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>`interface {{(redundant number</td>
<td>port-channel number</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>bridge-group number</code></td>
<td>Assigns the interface to a bridge group, where <code>number</code> is an integer between 1 and 100. You can assign up to four interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>nameif name</code></td>
<td>Names the interface. The <code>name</code> is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the <code>no</code> form, because that command causes all commands that refer to that name to be deleted.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>security-level number</code></td>
<td>Sets the security level, where <code>number</code> is an integer between 0 (lowest) and 100 (highest).</td>
</tr>
</tbody>
</table>

### What to Do Next

- (Optional) Configure a management interface. See [Configuring a Management Interface (ASA 5512-X and Higher and ASAv)](#) page 12-10.
- (Optional) Configure the MAC address and the MTU. See [Configuring the MAC Address, MTU, and TCP MSS](#) page 12-11.
- (Optional) Configure IPv6 addressing. See [Configuring IPv6 Addressing](#) page 12-14.
Configuring a Management Interface (ASA 5512-X and Higher and ASAv)

You can configure one management interface separate from the bridge group interfaces in single mode or per context. For more information, see Management Interface, page 9-2.

Restrictions

- See Management Interface, page 9-2.
- Do not assign this interface to a bridge group; a non-configurable bridge group (ID 101) is automatically added to your configuration. This bridge group is not included in the bridge group limit.
- If your model does not include a Management interface, you must manage the transparent firewall from a data interface; skip this procedure. (For example, on the ASASM.)
- In multiple context mode, you cannot share any interfaces, including the Management interface, across contexts. To provide management per context, you can create subinterfaces of the Management interface and allocate a Management subinterface to each context. Note that the ASA 5512-X through ASA 5555-X do not allow subinterfaces on the Management interface, so for per-context management, you must connect to a data interface.

Prerequisites

- Complete the procedures in Chapter 9, “Basic Interface Configuration (ASA Appliances).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the change to context name command.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> interface (port-channel number</td>
<td>management slot/port</td>
</tr>
<tr>
<td>Example: ciscoasa(config)# interface management 0/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> nameif name</td>
<td>Names the interface. The name is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the no form, because that command causes all commands that refer to that name to be deleted.</td>
</tr>
<tr>
<td>Example: ciscoasa(config-if)# nameif management</td>
<td></td>
</tr>
</tbody>
</table>
Completing Interface Configuration in Transparent Mode

**What to Do Next**

- (Optional) Configure the MAC address and the MTU. See Configuring the MAC Address, MTU, and TCP MSS, page 12-11.

## Configuring the MAC Address, MTU, and TCP MSS

This section describes how to configure MAC addresses for interfaces, how to set the MTU, and set the TCP MSS.

### Information About MAC Addresses

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

For the ASASM, all VLANs use the same MAC address provided by the backplane.

A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this command, then it is used regardless of the member interface MAC addresses.

### Command and Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip address ip_address [mask] [standby ip_address]</code></td>
<td>Sets the IP address manually. <strong>Note</strong> For use with failover, you must set the IP address and standby address manually; DHCP is not supported. The <code>ip_address</code> and <code>mask</code> arguments set the interface IP address and subnet mask. The <code>standby ip_address</code> argument is used for failover. See Configure Active/Standby Failover, page 7-25 or Configure Active/Active Failover, page 7-29 for more information.</td>
</tr>
<tr>
<td><code>ip address dhcp [setroute]</code></td>
<td>Obtains an IP address from a DHCP server. The <code>setroute</code> keyword lets the ASA use the default route supplied by the DHCP server. Reenter this command to reset the DHCP lease and request a new lease. If you do not enable the interface using the <code>no shutdown</code> command before you enter the <code>ip address dhcp</code> command, some DHCP requests might not be sent.</td>
</tr>
<tr>
<td><code>security-level number</code></td>
<td>Sets the security level, where <code>number</code> is an integer between 0 (lowest) and 100 (highest).</td>
</tr>
</tbody>
</table>

**Example:**

```bash
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

```bash
ciscoasa(config-if)# ip address dhcp
```

```bash
ciscoasa(config-if)# ip address dhcp setroute
```

```bash
ciscoasa(config-if)# security-level 50
```
Completing Interface Configuration in Transparent Mode

For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses the lowest numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can manually configure a MAC address for the port-channel interface. In multiple context mode, you can automatically assign unique MAC addresses to interfaces, including an EtherChannel port interface. We recommend manually, or in multiple context mode, automatically configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the ASA easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See How the ASA Classifies Packets, page 6-3 for more information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See Assign MAC Addresses to Context Interfaces Automatically, page 6-23 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use this procedure to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

Information About the MTU and TCP MSS

See Control Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size, page 9-7.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the changeto context name command.
- To increase the MTU above 1500, enable jumbo frames on supported models according to Enable Jumbo Frame Support, page 9-22. Jumbo frames are supported by default on the ASASM; you do not need to enable them.
### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you are not already in interface configuration mode, enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>For the ASA 5512-X and higher and the ASAv:</strong></td>
<td>The <code>redundant number</code> argument is the redundant interface ID, such as <code>redundant 1</code>.</td>
</tr>
<tr>
<td>`interface {{redundant number</td>
<td>port-channel number</td>
</tr>
<tr>
<td><code>mapped_name}}</code></td>
<td>See Enable the Physical Interface and Configure Ethernet Parameters, page 9-14 section for a description of the physical interface ID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Append the <code>subinterface</code> ID to the physical or redundant interface ID separated by a period (.).</td>
</tr>
<tr>
<td><code>ciscoasa(config)# interface vlan 100</code></td>
<td>In multiple context mode, enter the <code>mapped_name</code> if one was assigned using the <code>allocate-interface</code> command.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Assigns a private MAC address to this interface. The <code>mac_address</code> is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE.</td>
</tr>
<tr>
<td><code>mac-address mac_address [standby mac_address]</code></td>
<td>The first two bytes of a manual MAC address cannot be A2 if you also want to use auto-generated MAC addresses.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>For use with failover, set the <code>standby</code> MAC address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.</td>
</tr>
<tr>
<td><code>ciscoasa(config-if)# mac-address 000C.F142.4CDE</code></td>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><code>mtu interface_name bytes</code></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>For models that support jumbo frames, if you enter a value for any interface that is greater than 1500, then you need to enable jumbo frame support. See Enable Jumbo Frame Support, page 9-22.</td>
</tr>
<tr>
<td><code>ciscoasa(config)# mtu inside 9200</code></td>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><code>sysopt connection tcpmss [minimum] bytes</code></td>
<td>For the <code>minimum</code> keyword, sets the maximum segment size to be no less than <code>bytes</code>, between 48 and 65535. The minimum feature is disabled by default (set to 0).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config)# sysopt connection tcpmss minimum 1290</code></td>
<td></td>
</tr>
</tbody>
</table>
What to Do Next


Configuring IPv6 Addressing

This section describes how to configure IPv6 addressing.

- Information About IPv6, page 12-14
- Configuring a Global IPv6 Address, page 12-15
- Configuring IPv6 Neighbor Discovery, page 12-16

Information About IPv6

This section includes information about how to configure IPv6.

- IPv6 Addressing, page 12-14
- Modified EUI-64 Interface IDs, page 12-14
- Unsupported Commands, page 12-15

IPv6 Addressing

You can configure two types of unicast addresses for IPv6:

- Global—The global address is a public address that you can use on the public network. This address needs to be configured for each bridge group, and not per-interface. You can also configure a global IPv6 address for the management interface.

- Link-local—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the ND functions such as address resolution and neighbor discovery. Because the link-local address is only available on a segment, and is tied to the interface MAC address, you need to configure the link-local address per interface.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local addresses is automatically configured on each interface, so you do not also need to specifically configure a link-local address. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

**Note**

If you want to only configure the link-local addresses, see the `ipv6 enable` (to auto-configure) or `ipv6 address link-local` (to manually configure) command in the command reference.

Modified EUI-64 Interface IDs

RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture requires that the interface identifier portion of all unicast IPv6 addresses, except those that start with binary value 000, be 64 bits long and be constructed in Modified EUI-64 format. The ASA can enforce this requirement for hosts attached to the local link.
When this feature is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the IPv6 packets do not use the Modified EUI-64 format for the interface identifier, the packets are dropped and the following system log message is generated:

%ASA-3-325003: EUI-64 source address check failed.

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

Unsupported Commands

The following IPv6 commands are not supported in transparent firewall mode, because they require router capabilities:

- `ipv6 address autoconfig`
- `ipv6 nd prefix`
- `ipv6 nd ra-interval`
- `ipv6 nd ra-lifetime`
- `ipv6 nd suppress-ra`

Configuring a Global IPv6 Address

To configure a global IPv6 address for a bridge group or management interface, perform the following steps.

Note

Configuring the global address automatically configures the link-local address, so you do not need to configure it separately.

Restrictions

The ASA does not support IPv6 anycast addresses.

Prerequisites

- Set up your interfaces depending on your model:
  - ASA 5512-X and higher—Chapter 9, “Basic Interface Configuration (ASA Appliances).”
  - ASASM—ASASM quick start guide.
  - ASAv—Chapter 10, “Basic Interface Configuration (ASAv).”
- In multiple context mode, you can only configure context interfaces that you already assigned to the context in the system configuration according to Configure Multiple Contexts, page 6-14.
- In multiple context mode, complete this procedure in the context execution space. To change from the system to a context configuration, enter the `changeto context name` command.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you are not already in interface configuration mode, enters interface configuration mode.</td>
</tr>
<tr>
<td>For the bridge group:</td>
<td></td>
</tr>
<tr>
<td><code>interface bvi bridge_group_id</code></td>
<td></td>
</tr>
<tr>
<td>For the management interface:</td>
<td></td>
</tr>
<tr>
<td><code>interface management_interface_id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config)# interface bvi 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Assigns a global address to the interface. When you assign a global address, the link-local address is automatically created for the interface (for a bridge group, for each member interface).</td>
</tr>
<tr>
<td>IPv6 address IPv6-address/prefix-length [standby IPv6-address]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enforces the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link.</td>
</tr>
<tr>
<td>(Optional) IPv6 enforce-eui64 if_name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config)# ipv6 enforce-eui64 inside</code></td>
<td></td>
</tr>
</tbody>
</table>

Configuring IPv6 Neighbor Discovery


Allowing Same Security Level Communication

By default, interfaces on the same security level cannot communicate with each other, and packets cannot enter and exit the same interface. This section describes how to enable inter-interface communication when interfaces are on the same security level.

Information About Inter-Interface Communication

Allowing interfaces on the same security level to communicate with each other is useful if you want traffic to flow freely between all same security interfaces without ACLs.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>same-security-traffic permit inter-interface</td>
<td>Enables interfaces on the same security level so that they can communicate with each other.</td>
</tr>
</tbody>
</table>

Turning Off and Turning On Interfaces

This section describes how to turn off and on an interface.

All interfaces are enabled by default. In multiple context mode, if you disable or reenable the interface within a context, only that context interface is affected. But if you disable or reenable the interface in the system execution space, then you affect that interface for all contexts.

Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ciscoasa(config)# interface (vlan number</td>
<td>If you are not already in interface configuration mode, enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>mapped_name)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>In multiple context mode, enter the mapped_name if one was assigned using the allocate-interface command.</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config)# interface vlan 100</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>shutdown</td>
<td>Disables the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# shutdown</td>
<td>Reenables the interface.</td>
</tr>
<tr>
<td>3</td>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface</td>
<td>Displays interface statistics.</td>
</tr>
<tr>
<td>show interface ip brief</td>
<td>Displays interface IP addresses and status.</td>
</tr>
<tr>
<td>show bridge-group</td>
<td>Shows bridge group information.</td>
</tr>
</tbody>
</table>
The following example includes two bridge groups of three interfaces each, plus a management-only interface:

```plaintext
interface gigabitethernet 0/0
    nameif inside1
    security-level 100
    bridge-group 1
    no shutdown
interface gigabitethernet 0/1
    nameif outside1
    security-level 0
    bridge-group 1
    no shutdown
interface gigabitethernet 0/2
    nameif dmz1
    security-level 50
    bridge-group 1
    no shutdown
interface bvi 1
    ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
interface gigabitethernet 1/0
    nameif inside2
    security-level 100
    bridge-group 2
    no shutdown
interface gigabitethernet 1/1
    nameif outside2
    security-level 0
    bridge-group 2
    no shutdown
interface gigabitethernet 1/2
    nameif dmz2
    security-level 50
    bridge-group 2
    no shutdown
interface bvi 2
    ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
interface management 0/0
    nameif mgmt
    security-level 100
    ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
    no shutdown
```
# Feature History for Transparent Mode Interfaces

Table 12-1 lists each feature change and the platform release in which it was implemented.

### Table 12-1  Feature History for Interfaces in Transparent Mode

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased VLANs</td>
<td>7.0(5)</td>
<td>Increased the following limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Base license VLANs from 0 to 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Security Plus license VLANs from 10 to 25.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5520 VLANs from 25 to 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5540 VLANs from 100 to 200.</td>
</tr>
<tr>
<td>Increased VLANs</td>
<td>7.2(2)</td>
<td>The maximum number of VLANs for the Security Plus license on the ASA 5505 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 backup interface command is still useful for an Easy VPN configuration. VLAN limits were also increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), the ASA 5550 (from 200 to 250).</td>
</tr>
<tr>
<td>Gigabit Ethernet Support for the ASA 5510 Security Plus License</td>
<td>7.2(3)</td>
<td>The ASA 5510 now supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports 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 <code>speed</code> command to change the speed on the interface and use the <code>show interface</code> command to see what speed is currently configured for each interface.</td>
</tr>
<tr>
<td>Native VLAN support for the ASA 5505</td>
<td>7.2(4)/8.0(4)</td>
<td>You can now include the native VLAN in an ASA 5505 trunk port. We introduced the following command: <code>switchport trunk native vlan</code>.</td>
</tr>
</tbody>
</table>
Table 12-1  Feature History for Interfaces in Transparent Mode (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Jumbo packet support for the ASA 5580                                        | 8.1(1)            | The Cisco ASA 5580 supports jumbo frames. 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 maximum use of other features, such as ACLs.
We introduced the following command: **jumbo-frame reservation**. |
| Increased VLANs for the ASA 5580                                             | 8.1(2)            | The number of VLANs supported on the ASA 5580 are increased from 100 to 250.                                                                           |
| IPv6 support for transparent mode                                            | 8.2(1)            | IPv6 support was introduced for transparent firewall mode.                                                                                               |
| Support for Pause Frames for Flow Control on the ASA 5580 10-Gigabit Ethernet Interfaces | 8.2(2)            | You can now enable pause (XOFF) frames for flow control. We introduced the following command: **flowcontrol**.                                      |
| Bridge groups for transparent mode                                          | 8.4(1)            | 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 eight bridge groups of four interfaces each in single mode or per context. We introduced the following commands: **interface bvi, show bridge-group**. |
| Transparent mode bridge group maximum increased to 250                      | 9.3(1)            | The bridge group maximum was increased from 8 to 250 bridge groups. You can configure up to 250 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group. We modified the following commands: **interface bvi, bridge-group**. |
Traffic Zones

You can assign multiple interfaces to a traffic zone, which lets traffic from an existing flow exit or enter the ASA on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the ASA as well as external load balancing of traffic to the ASA across multiple interfaces.

- About Traffic Zones, page 13-1
- Prerequisites for Traffic Zones, page 13-7
- Guidelines for Traffic Zones, page 13-8
- Configure a Traffic Zone, page 13-9
- Monitoring Traffic Zones, page 13-10
- Example for Traffic Zones, page 13-12
- History for Traffic Zones, page 13-15

About Traffic Zones

- Non-Zoned Behavior, page 13-2
- Why Use Zones?, page 13-2
- Per-Zone Connection and Routing Tables, page 13-4
- ECMP Routing, page 13-4
- Interface-Based Security Policy, page 13-5
- Supported Services for Traffic Zones, page 13-6
- Security Levels, page 13-6
- Primary and Current Interface for the Flow, page 13-6
- Joining or Leaving a Zone, page 13-6
- Intra-Zone Traffic, page 13-6
- To- and From-the-Box Traffic, page 13-7
- Overlapping IP Addresses Within a Zone, page 13-7
Non-Zoned Behavior

The Adaptive Security Algorithm (Stateful Inspection Overview, page 1-13) takes into consideration the state of a packet when deciding to permit or deny the traffic. One of the enforced parameters for the flow is that traffic enters and exits the same interface. Any traffic for an existing flow that enters a different interface is dropped by the ASA.

Traffic zones let you group multiple interfaces together so that traffic entering or exiting any interface in the zone fulfills the Adaptive Security Algorithm security checks.

Why Use Zones?

- Asymmetric Routing, page 13-2
- Lost Route, page 13-3
- Load Balancing, page 13-3

Asymmetric Routing

In the following scenario, a connection was established between an inside host and an outside host through ISP 1 on the Outside1 interface. Due to asymmetric routing on the destination network, return traffic arrived from ISP 2 on the Outside2 interface.

Non-Zoned Problem: The ASA maintains the connection tables on a per-interface basis. When the returning traffic arrives at Outside2, it will not match the connection table and will be dropped.
**Zoned Solution**: The ASA maintains connection tables on a per-zone basis. If you group Outside1 and Outside2 into a zone, then when the returning traffic arrives at Outside2, it will match the per-zone connection table, and the connection will be allowed.

**Lost Route**

In the following scenario, a connection was established between an inside host and an outside host through ISP 1 on the Outside1 interface. Due to a lost or moved route between Outside1 and ISP 1, traffic needs to take a different route through ISP 2.

**Non-Zoned Problem**: The connection between the inside and outside host will be deleted; a new connection must be established using a new next-best route. For UDP, the new route will be used after a single packet drop, but for TCP, a new connection has to be reestablished.

**Zoned Solution**: The ASA detects the lost route and switches the flow to the new path through ISP 2. Traffic will be seamlessly forwarded without any packet drops.

**Load Balancing**

In the following scenario, a connection was established between an inside host and an outside host through ISP 1 on the Outside1 interface. A second connection was established through an equal cost route through ISP 2 on Outside2.
About Traffic Zones

**Non-Zoned Problem**: Load-balancing across interfaces is not possible; you can only load-balance with equal cost routes on one interface.

**Zoned Solution**: The ASA load-balances connections across up to eight equal cost routes on all the interfaces in the zone.

**Per-Zone Connection and Routing Tables**

The ASA maintains a per-zone connection table so that traffic can arrive on any of the zone interfaces. The ASA also maintains a per-zone routing table for ECMP support.

**ECMP Routing**

- The ASA supports Equal-Cost Multi-Path (ECMP) routing.
- **Non-Zoned ECMP Support**, page 13-4
- **Zoned ECMP Support**, page 13-5
- **How Connections Are Load-Balanced**, page 13-5
- **Falling Back to a Route in Another Zone**, page 13-5

**Non-Zoned ECMP Support**

Without zones, you can have up to 3 equal cost static or dynamic routes per interface. For example, you can configure three default routes on the outside interface that specify different gateways:
Chapter 13      Traffic Zones

About Traffic Zones

route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4

In this case, traffic is load-balanced on the outside interface between 10.1.1.2, 10.1.1.3, and 10.1.1.4. Traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses.

ECMP is not supported across multiple interfaces, so you cannot define a route to the same destination on a different interface. The following route is disallowed when configured with any of the routes above:
route outside2 0 0 10.2.1.1

Zoned ECMP Support

With zones, you can have up to 8 equal cost static or dynamic routes across up to 8 interfaces within a zone. For example, you can configure three default routes across three interfaces in the zone:
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2

Similarly, your dynamic routing protocol can automatically configure equal cost routes. The ASA load-balances traffic across the interfaces with a more robust load balancing mechanism.

When a route is lost, the ASA seamlessly moves the flow to a different route.

How Connections Are Load-Balanced

The ASA load balances connections across equal cost routes using a hash made from the packet 6-tuple (source and destination IP address, source and destination port, protocol, and ingress interface). Unless the route is lost, a connection will stay on the chosen interface for its duration.

Packets within a connection are not load-balanced across routes; a connection uses a single route unless that route is lost.

The ASA does not consider the interface bandwidth or other parameters when load balancing. You should make sure all interfaces within the same zone have the same characteristics such as MTU, bandwidth, and so on.

The load-balancing algorithm is not user configurable.

Falling Back to a Route in Another Zone

When a route is lost on an interface, if there are no other routes available within the zone, then the ASA will use a route from a different interface/zone. If this backup route is used, then you may experience packet drops as with non-zoned routing support.

Interface-Based Security Policy

Zones allow traffic to and from any interface in the zone, but the security policy itself (access rules, NAT, and so on) is still applied per interface, not per zone. If you configure the same security policy for all interfaces within the zone, then you can successfully implement ECMP and load balancing for that traffic. For more information about required parallel interface configuration, see Prerequisites for Traffic Zones, page 13-7.
Supported Services for Traffic Zones

The following services are supported with zones:

- Access Rules
- NAT
- Service Rules, except for QoS traffic policing.
- Routing

You can also configure to- and from-the-box services listed in To- and From-the-Box Traffic, page 13-7, although full zoned support is not available.

Do not configure other services (such as VPN or Botnet Traffic Filter) for interfaces in a traffic zone; they may not function or scale as expected.

Note

For detailed information about how to configure the security policy, see Prerequisites for Traffic Zones, page 13-7.

Security Levels

The first interface that you add to a zone determines the security level of the zone. All additional interfaces must have the same security level. To change the security level for interfaces in a zone, you must remove all but one interface, and then change the security levels, and re-add the interfaces.

Primary and Current Interface for the Flow

Each connection flow is built based on the initial ingress and egress interfaces. These interfaces are the primary interfaces.

If a new egress interface is used because of route changes or asymmetric routing, then the new interfaces are the current interfaces.

Joining or Leaving a Zone

When you assign an interface to a zone, any connections on that interface are deleted. The connections must be reestablished.

If you remove an interface from a zone, any connections that have the interface as the primary interface are deleted. The connections must be reestablished. If the interface is the current interface, the ASA moves the connections back to the primary interface. The zone route table is also refreshed.

Intra-Zone Traffic

To allow traffic to enter one interface and exit another in the same zone, enable the same-security permit intra-interface command, which allows traffic to enter and exit the same interface, as well as the same-security permit inter-interface command, which allows traffic between same-security interfaces. Otherwise, a flow cannot be routed between two interfaces in the same zone.
To- and From-the-Box Traffic

- You cannot add management-only or management-access interfaces to a zone.
- For management traffic on regular interfaces in a zone, only asymmetric routing on existing flows is supported; there is no ECMP support.
- You can configure a management service on only one zone interface, but to take advantage of asymmetric routing support, you need to configure it on all interfaces. Even when the configurations are parallel on all interfaces, ECMP is not supported.
- The ASA supports the following to- and from-the-box services in a zone:
  - Telnet
  - SSH
  - HTTPS
  - SNMP
  - Syslog
  - BGP

Overlapping IP Addresses Within a Zone

For non-zoned interfaces, the ASA supports overlapping IP address networks on interfaces so long as you configure NAT properly. However, overlapping networks are not supported on interfaces in the same zone.

Prerequisites for Traffic Zones

- Configure all interface parameters including the name, IP address, and security level. Note that the security level must match for all interfaces in the zone. You should plan to group together like interfaces in terms of bandwidth and other Layer 2 properties.
- Configure the following services to match on all zone interfaces:
  - Access Rules—Apply the same access rule to all zone member interfaces, or use a global access rule.
    
    For example:
    
    ```
    access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
    access-group ZONE1 in interface outside1
    access-group ZONE1 in interface outside2
    access-group ZONE1 in interface outside3
    ```
  - NAT—Configure the same NAT policy on all member interfaces of the zone or use a global NAT rule (in other words, use “any” to represent the zone interfaces in the NAT rule).

    Interface PAT is not supported.

    For example:
    
    ```
    object network WEBSERVER1
    host 10.9.9.9 255.255.255.255
    nat (inside, any) static 209.165.201.9
    ```
Guidelines for Traffic Zones

Firewall Mode
Supported in routed firewall mode only. Does not support transparent firewall mode.

Failover
- You cannot add the failover or state link to a zone.
- In Active/Active failover mode, you can assign an interface in each context to an asymmetrical routing (ASR) group. This service allows traffic returning on a similar interface on the peer unit to be restored to the original unit. You cannot configure both ASR groups and traffic zones within a context. If you configure a zone in a context, none of the context interfaces can be part of an ASR group. See Configure Support for Asymmetrically Routed Packets (Active/Active Mode), page 7-38 for more information about ASR groups.
- Only the primary interfaces for each connection are replicated to the standby unit; current interfaces are not replicated. If the standby unit becomes active, it will assign a new current interface if necessary.
Configure a Traffic Zone

Configure a named zone, and assign interfaces to the zone.

Procedure

**Step 1** Add the zone:

```
zone name
```

For example:

```
zone outside
```

The zone name can be up to 48 characters in length.

**Step 2** Add an interface to the zone:

```
interface id
zone-member zone_name
```

For example:

```
interface gigabitethernet0/0
zone-member outside
```

**Step 3** Add more interfaces to the zone; ensure they have the same security level as the first interface you added.

For example:
Monitoring Traffic Zones

- Zone Information, page 13-10
- Zone Connections, page 13-11
- Zone Routing, page 13-11

Zone Information

- **show zone [name]**
  Shows zone ID, context, security level, and members.
  See the following output for the `show zone` command:

```plaintext
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**
  Shows the interface names and zone names.
  See the following output for the `show nameif zone` command:

```plaintext
ciscoasa# show nameif zone

Interface    Name               zone-name       Security
------------- -------------------- --------------- ----------
GigabitEthernet0/0 inside-1     inside-zone    100
GigabitEthernet0/1.21 inside     inside-zone    100
GigabitEthernet0/1.31 4 inside-zone 0
GigabitEthernet0/2 outside     outside-zone  0
```
Zone Connections

- **show conn [long | detail] [zone zone_name [zone zone_name] [...]]**
  The **show conn zone** command displays connections for a zone. The **long** and **detail** keywords show the primary interface on which the connection was built and the current interface used to forward the traffic.

  See the following output for the **show conn long zone** command:
  
  ```
  ciscoasa# show conn long zone zone-inside zone zone-outside
  TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
  ```

- **show asp table zone**
  Shows the accelerated security path tables for debugging purposes.

- **show local-host [zone zone_name [zone zone_name] [...]]**
  Shows the network states of local hosts within a zone.

  See the following output for the **show local-host zone** command. The primary interface is listed first, and the current interface is in parentheses.

  ```
  ciscoasa# show local-host zone outside-zone
  Zone:outside-zone: 4 active, 5 maximum active, 0 denied
  local host: <10.122.122.1>,
  TCP flow count/limit = 3/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited
  Conn: 
  TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
  ```

Zone Routing

- **show route zone**
  Shows the routes for zone interfaces.

  See the following output for the **show route zone** command:

  ```
  ciscoasa# show route zone
  Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
  D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
  E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
  i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
  * - candidate default, U - per-user static route, o - ODR
  P - periodic downloaded static route
  Gateway of last resort is not set
  ```
Example for Traffic Zones

The following example assigns 4 VLAN interfaces to the outside zone, and configures 4 equal cost default routes. PAT is configured for the inside interface, and a web server is available on a DMZ interface using static NAT.
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch
zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown
interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87

# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
## History for Traffic Zones

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Zones</td>
<td>9.3(2)</td>
<td>You can group interfaces together into a traffic zone to accomplish traffic load balancing (using Equal Cost Multi-Path (ECMP) routing), route redundancy, and asymmetric routing across multiple interfaces. <strong>Note</strong> You cannot apply a security policy to a named zone; the security policy is interface-based. When interfaces in a zone are configured with the same access rule, NAT, and service policy, then load-balancing and asymmetric routing operate correctly. We introduced or modified the following commands: <code>zone</code>, <code>zone-member</code>, <code>show running-config zone</code>, <code>clear configure zone</code>, <code>show zone</code>, <code>show asp table zone</code>, <code>show nameif zone</code>, <code>show conn long</code>, <code>show local-host zone</code>, <code>show route zone</code>, <code>show asp table routing</code>, <code>clear conn zone</code>, <code>clear local-host zone</code></td>
</tr>
</tbody>
</table>

- inspect rtsp
- inspect skinny
- inspect esmtp_default_esmtp_map
- inspect sqlnet
- inspect sunrpc
- inspect tftp
- inspect sip
- inspect xdmcp

service-policy global_policy global
PART 4

Basic Settings
Basic Settings

This chapter describes how to configure basic settings on the ASA that are typically required for a functioning configuration.

- Set the Hostname, Domain Name, and the Enable and Telnet Passwords, page 14-1
- Recover Enable and Telnet Passwords, page 14-3
- Set the Date and Time, page 14-7
- Configure the Master Passphrase, page 14-10
- Configure the DNS Server, page 14-14
- Monitoring the DNS Cache, page 14-16
- History for Basic Settings, page 14-17

Set the Hostname, Domain Name, and the Enable and Telnet Passwords

This section describes how to configure the hostname, domain name, and the enable and Telnet passwords.

**Before You Begin**
- In multiple context mode, you can configure the hostname and domain name in both the system and context execution spaces.
- For the enable and Telnet passwords, set them in each context; they are not available in the system. When you session to the ASASM from the switch in multiple context mode, the ASASM uses the login password you set in the admin context.
- To change from the system to a context configuration, enter the `changeto context name` command.

To set the hostname, domain name, and the enable and Telnet passwords, perform the following steps.

**Procedure**

**Step 1** Specify the hostname for the ASA or for a context. The default hostname is “asa.”

```bash
hostname name
```
Set the Hostname, Domain Name, and the Enable and Telnet Passwords

Example:

ciscoasa(config)# hostname myhostnameexample12345

This name can be up to 63 characters. The hostname must start and end with a letter or digit, and have only letters, digits, or a hyphen.

When you set a hostname for the ASA, that name appears in the command line prompt. If you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands.

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line, but can be used by the `banner` command `$(hostname)` token.

Step 2 Specify the domain name for the ASA. The default domain name is default.domain.invalid.

domain-name name

Example:

ciscoasa(config)# domain-name example.com

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com” and specify a syslog server by the unqualified name of “jupiter,” then the ASA qualifies the name to “jupiter.example.com.”

Step 3 Change the enable password. By default, the enable password is blank.

The enable password lets you enter privileged EXEC mode if you do not configure enable authentication. The enable password also lets you log into ASDM with a blank username if you do not configure HTTP authentication.

`enable password password`

Example:

ciscoasa(config)# enable passwd Pa$$w0rd

The `password` argument is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

This command changes the password for the highest privilege level (15). If you configure local command authorization, you can set enable passwords for each privilege level from 0 to 15 using the following syntax:

`enable password password level number`

The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. Enter the `enable password` command without a password to set the password to the default, which is blank.

Step 4 Set the login password for Telnet access. There is no default password.

The login password is used for Telnet access when you do not configure Telnet authentication. You also use this password when accessing the ASASM from the switch with the `session` command.

`{passwd | password} password [encrypted]`

Example:

ciscoasa(config)# password cisco12345

You can enter `passwd` or `password`. The `password` is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.
Recover Enable and Telnet Passwords

If you forget the enable or Telnet passwords, you can recover them. The procedure differs by device type. You must perform the task using the CLI.

Recover Passwords on the ASA

To recover passwords for the ASA, perform the following steps:

Procedure

**Step 1** Connect to the ASA console port.

**Step 2** Power off the ASA, then power it on.

**Step 3** After startup, press the **Escape** key when you are prompted to enter ROMMON mode.

**Step 4** To update the configuration register value, enter the following command:

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

**Step 5** To set the ASA to ignore the startup configuration, enter the following command:

```
rommon #1> confreg
```

The ASA displays the current configuration register value, and asks whether you want to change it:

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

**Step 6** Record the current configuration register value, so you can restore it later.

**Step 7** At the prompt, enter **Y** to change the value. The ASA prompts you for new values.

**Step 8** Accept the default values for all settings, except for the "disable system configuration?" value.

**Step 9** At the prompt, enter **Y**.

**Step 10** Reload the ASA by entering the following command:

```
rommon #2> boot
```
Chapter 14      Basic Settings

Recover Enable and Telnet Passwords

Step 11 Access the privileged EXEC mode by entering the following command:

```
ciscoasa# enable
```

Step 12 When prompted for the password, press Enter.

The password is blank.

Step 13 Load the startup configuration by entering the following command:

```
ciscoasa# copy startup-config running-config
```

Step 14 Access the global configuration mode by entering the following command:

```
ciscoasa# configure terminal
```

Step 15 Change the passwords, as required, in the default configuration by entering the following commands:

```
ciscoasa(config)# password password
```
```
ciscoasa(config)# enable password password
```
```
ciscoasa(config)# username name password password
```

Step 16 Load the default configuration by entering the following command:

```
ciscoasa(config)# no config-register
```

The default configuration register value is 0x1. See the command reference for more information about the configuration register.

Step 17 Save the new passwords to the startup configuration by entering the following command:

```
ciscoasa(config)# copy running-config startup-config
```

---

Recover Passwords on the ASA 5506-X

To recover passwords for the ASA 5506-X, perform the following steps:

**Procedure**

Step 1 Connect to the ASA console port.

Step 2 Power off the ASA, then power it on.

Step 3 After startup, press the Escape key when you are prompted to enter ROMMON mode.

Step 4 To update the configuration register value, enter the following command:

```
rommon #1> confreg 0x41
```

You must reset or power cycle for new config to take effect.

The ASA displays the current configuration register value and a list of configuration options. Record the current configuration register value, so you can restore it later.

Configuration Register: 0x00000041
Configuration Summary
[ 0 ] password recovery
[ 1 ] display break prompt
[ 2 ] ignore system configuration
[ 3 ] auto-boot image in disks
boot: ...... auto-boot index 1 image in disks

Step 5  Reload the ASA by entering the following command:

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...

The ASA loads the default configuration instead of the startup configuration.

Step 6  Access the privileged EXEC mode by entering the following command:
ciscoasa# enable

Step 7  When prompted for the password, press Enter.
The password is blank.

Step 8  Load the startup configuration by entering the following command:
ciscoasa# copy startup-config running-config

Step 9  Access the global configuration mode by entering the following command:
ciscoasa# configure terminal

Step 10 Change the passwords, as required, in the default configuration by entering the following commands:
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password

Step 11 Load the default configuration by entering the following command:
ciscoasa(config)# no config-register

The default configuration register value is 0x1. See the command reference for more information about the configuration register.

Step 12 Save the new passwords to the startup configuration by entering the following command:
ciscoasa(config)# copy running-config startup-config

---

Recover Passwords or Images on the ASAv

To recover passwords or images on the ASAv, perform the following steps:

Procedure

Step 1  Copy the running configuration to a backup file on the ASAv:
copy running-config filename
Example:
ciscoasa# copy running-config backup.cfg

**Step 2**  
Restart the ASAv:
```
reload
```

**Step 3**  
From the GNU GRUB menu, press the down arrow, choose the `<filename> with no configuration load` option, then press **Enter**. The filename is the default boot image filename on the ASAv. The default boot image is never automatically booted through the `fallback` command. Then load the selected boot image.

GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
`bootflash: /asa100123-20-smp-k8.bin with no configuration load`

Example:
```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin with no configuration load
```

**Step 4**  
Copy the backup configuration file to the running configuration.
```
copy filename running-config
```

Example:
ciscoasa (config)# copy backup.cfg running-config

**Step 5**  
Reset the password.
```
enable password
```

Example:
ciscoasa(config)# enable password cisco123

**Step 6**  
Save the new configuration.
```
write memory
```

Example:
ciscoasa(config)# write memory

---

## Disable Password Recovery

**Note**  
You cannot disable password recovery on the ASAv.

To disable password recovery to ensure that unauthorized users cannot use the password recovery mechanism to compromise the ASA, perform the following steps.

**Before You Begin**  
On the ASA, the **no service password-recovery** command prevents you from entering ROMMON mode with the configuration intact. When you enter ROMMON mode, the ASA prompts you to erase all Flash file systems. You cannot enter ROMMON mode without first performing this erasure. If you choose not to erase the Flash file system, the ASA reloads. Because password recovery depends on using ROMMON
mode and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to restore the system to an operating state, load a new image and a backup configuration file, if available.

The service password-recovery command appears in the configuration file for information only. When you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the ASA is configured to ignore the startup configuration at startup (in preparation for password recovery), then the ASA changes the setting to load the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the no service password-recovery command replicates to the standby unit.

Procedure

Step 1 Disable password recovery.

no service password-recovery

Example:
ciscoasa (config)# no service password-recovery

---

Set the Date and Time

Note Do not set the date and time for the ASASM; it receives these settings from the host switch.

Set the Time Zone and Daylight Savings Dates

To set the time zone and date range, perform the following steps:

Procedure

Step 1 Set the time zone. By default, the time zone is UTC and the daylight saving time date range is from 2:00 a.m. on the first Sunday in April to 2:00 a.m. on the last Sunday in October.

clock timezone zone [-]hours [minutes]

Example:
ciscoasa(config)# clock timezone PST -8

The zone argument specifies the time zone as a string, for example, PST for Pacific Standard Time. The [-]hours value sets the number of hours of offset from UTC. For example, PST is -8 hours. The minutes value sets the number of minutes of offset from UTC.
Step 2 Enter one of the following commands to change the date range for daylight saving time from the default. The default recurring date range is from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

- Set the start and end dates for daylight saving time as a specific date in a specific year. If you use this command, you need to reset the dates every year.

  `clock summer-time zone date {day month | month day} year hh:mm (day month | month day) year hh:mm [offset]`

  Example:
  `ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60`

  The `zone` value specifies the time zone as a string, for example, PDT for Pacific Daylight Time.
  The `day` value sets the day of the month, from 1 to 31. You can enter the day and month as April 1 or as 1 April, for example, depending on your standard date format.
  The `month` value sets the month as a string. You can enter the day and month as April 1 or as 1 April, depending on your standard date format.
  The `year` value sets the year using four digits, for example, 2004. The year range is 1993 to 2035.
  The `hh:mm` value sets the hour and minutes in 24-hour time.
  The `offset` value sets the number of minutes to change the time for daylight saving time. By default, the value is 60 minutes.

- Specify the start and end dates for daylight saving time, in the form of a day and time of the month, and not a specific date in a year. This command enables you to set a recurring date range that you do not need to change yearly.

  `clock summer-time zone recurring [week weekday month hh:mm week weekday month hh:mm] [offset]`

  Example:
  `ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60`

  The `zone` value specifies the time zone as a string, for example, PDT for Pacific Daylight Time.
  The `week` value specifies the week of the month as an integer between 1 and 4 or as the words first or last. For example, if the day might fall in the partial fifth week, then specify last.
  The `weekday` value specifies the day of the week: Monday, Tuesday, Wednesday, and so on.
  The `month` value sets the month as a string.
  The `hh:mm` value sets the hour and minutes in 24-hour time.
  The `offset` value sets the number of minutes to change the time for daylight savings time. By default, the value is 60 minutes.

---

**Set the Date and Time Using an NTP Server**

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum—a measure of how reliable the data is.

Time derived from an NTP server overrides any time set manually.
Before You Begin
In multiple context mode, you can set the time in the system configuration only.
To set the date and time using an NTP server, perform the following steps:

Procedure

Step 1  Enable authentication with an NTP server.
ntp authenticate

Example:
ciscoasa(config)# ntp authenticate

Step 2  Specify an authentication key ID to be a trusted key, which is required for authentication with an NTP server.
ntp trusted-key key_id

Example:
ciscoasa(config)# ntp trusted-key 1

The key_id argument is a value between 1 and 4294967295. You can enter multiple trusted keys for use with multiple servers.

Step 3  Set a key to authenticate with an NTP server.
ntp authentication-key key_id md5 key

Example:
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey

The key_id argument is the ID that you set in Step 2 using the ntp trusted-key command, and the key argument is a string up to 32 characters long.

Step 4  Identify an NTP server.
ntp server ip_address [key key_id] [source interface_name] [prefer]

Example:
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer

The key_id argument is the ID that you set using the ntp trusted-key command.
The source interface_name keyword-argument pair identifies the outgoing interface for NTP packets if you do not want to use the default interface in the routing table. Because the system does not include any interfaces in multiple context mode, specify an interface name defined in the admin context.
The prefer keyword sets this NTP server as the preferred server if multiple servers have similar accuracy. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the prefer keyword specifies which of those servers to use. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one. For example, the ASA uses a server of stratum 2 over a server of stratum 3 that is preferred. You can identify multiple servers; the ASA uses the most accurate server.
Set the Date and Time Manually

This section describes how to set the date and time manually.

Before You Begin

In multiple context mode, you can set the time in the system configuration only.

To set the date and time manually, perform the following steps:

Procedure

Step 1

Set the date time manually.

```
clock set hh:mm:ss (month day | day month) year
```

Example:

```
ciscoasa# clock set 20:54:00 april 1 2004
```

The `hh:mm:ss` argument sets the hour, minutes, and seconds in 24-hour time. For example, enter 20:54:00 for 8:54 pm.

The day value sets the day of the month, from 1 to 31. You can enter the day and month as april 1 or as 1 april, for example, depending on your standard date format.

The month value sets the month. Depending on your standard date format, you can enter the day and month as april 1 or as 1 april.

The year value sets the year using four digits, for example, 2004. The year range is from 1993 to 2035.

The default time zone is UTC. If you change the time zone after you enter the `clock set` command using the `clock timezone` command, the time automatically adjusts to the new time zone.

This command sets the time in the hardware chip, and does not save the time in the configuration file. This time endures reboots. Unlike the other `clock` commands, this command is a privileged EXEC command. To reset the clock, you need to set a new time with the `clock set` command.

Configure the Master Passphrase

The master passphrase allows you to securely store plain text passwords in encrypted format and provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. Features that use the master passphrase include the following:

- OSPF
- EIGRP
- VPN load balancing
- VPN (remote access and site-to-site)
- Failover
- AAA servers
- Logging
- Shared licenses
Add or Change the Master Passphrase

This section describes how to add or change the master passphrase.

Before You Begin
This procedure will only be accepted in a secure session, for example by console, SSH, or ASDM via HTTPS.

To add or change the master passphrase, perform the following steps:

Procedure

Step 1
Set the passphrase used for generating the encryption key. The passphrase must be between 8 and 128 characters long. All characters except a backspace and double quotes are accepted for the passphrase. If you do not enter the new passphrase in the command, you are prompted for it. To change the passphrase, you must enter the old passphrase.

```
key config-key password-encryption [new_passphrase [old_passphrase]]
```

Example:
```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

Note  Use the interactive prompts to enter passwords to avoid having the passwords logged in the command history buffer.

Use the `no key config-key password-encrypt` command with caution, because it changes the encrypted passwords into plain text passwords. You may use the `no` form of this command when downgrading to a software version that does not support password encryption.

Step 2
Enable password encryption.

```
password encryption aes
```

Example:
```
ciscoasa(config)# password encryption aes
```

As soon as password encryption is enabled and the master passphrase is available, all the user passwords will be encrypted. The running configuration will show the passwords in the encrypted format.

If the passphrase is not configured at the time that password encryption is enabled, the command will succeed in anticipation that the passphrase will be available in the future.

If you later disable password encryption using the `no password encryption aes` command, all existing encrypted passwords are left unchanged, and as long as the master passphrase exists, the encrypted passwords will be decrypted, as required by the application.
Step 3  Save the runtime value of the master passphrase and the resulting configuration.

write memory

Example:
ciscoasa(config)# write memory

If you do not enter this command, passwords in startup configuration may still be visible if they were not saved with encryption previously. In addition, in multiple context mode the master passphrase is changed in the system context configuration. As a result, the passwords in all contexts will be affected. If the write memory command is not entered in the system context mode, but not in all user contexts, then the encrypted passwords in user contexts may be stale. Alternatively, use the write memory all command in the system context to save all configurations.

Examples
The following example shows that no previous key was present:
ciscoasa(config)# key config-key password-encryption 12345678

The following example shows that a key already exists:
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678

In the following example, you enter the command without parameters so that you will be prompted for keys. Because a key already exists, you are prompted for it.
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789

In the following example, there is no existing key, so you are not prompted to supply it.
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678

Disable the Master Passphrase

Disabling the master passphrase reverts encrypted passwords into plain text passwords. Removing the passphrase might be useful if you downgrade to a previous software version that does not support encrypted passwords.

Before You Begin

- You must know the current master passphrase to disable it. See Remove the Master Passphrase, page 14-13 if you do not know the passphrase.

- This procedure works only in a secure session; that is, by Telnet, SSH, or ASDM via HTTPS.

To disable the master passphrase, perform the following steps:
Configure the Master Passphrase

**Procedure**

**Step 1**  
Remove the master passphrase. If you do not enter the passphrase in the command, you are prompted for it.

```powershell
no key config-key password-encryption [old_passphrase]
```

Example:

```
ciscoasa(config)# no key config-key password-encryption
```

Warning! You have chosen to revert the encrypted passwords to plain text. This operation will expose passwords in the configuration and therefore exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee

**Step 2**  
Save the runtime value of the master passphrase and the resulting configuration.

```powershell
write memory
```

Example:

```
ciscoasa(config)# write memory
```

The non-volatile memory containing the passphrase will be erased and overwritten with the 0xFF pattern.

In multiple mode, the master passphrase is changed in the system context configuration. As a result, the passwords in all contexts will be affected. If the `write memory` command is entered in the system context mode, but not in all user contexts, then the encrypted passwords in user contexts may be stale. Alternatively, use the `write memory all` command in the system context to save all configurations.

---

**Remove the Master Passphrase**

You cannot recover the master passphrase. If the master passphrase is lost or unknown, you can remove it.

**Procedure**

**Step 1**  
Remove the master key and the configuration that includes the encrypted passwords.

```powershell
write erase
```

Example:

```
ciscoasa(config)# write erase
```

**Step 2**  
Reload the ASA with the startup configuration, without any master key or encrypted passwords.

```powershell
reload
```

Example:

```
ciscoasa(config)# reload
```
Configure the DNS Server

You need to configure DNS servers so that the ASA can resolve host names to IP addresses. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database. Other features, such as the ping or traceroute command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names.

Note
The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the name command to associate a name with an IP address and enable use of the names using the names command.

Before You Begin
Make sure that you configure the appropriate routing and access rules for any interface on which you enable DNS domain lookup so you can reach the DNS server.

To configure the DNS server, perform the following steps:

Procedure

Step 1
Enable the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.

```
dns domain-lookup interface_name
```

Example:
```
ciscoasa(config)# dns domain-lookup inside
```

Step 2
Specify the DNS server group that the ASA uses for outgoing requests.

```
dns server-group DefaultDNS
```

Example:
```
ciscoasa(config)# dns server-group DefaultDNS
```

Other DNS server groups can be configured for VPN tunnel groups. See the tunnel-group command in the command reference for more information.

Step 3
Specify one or more DNS servers. You may enter all six IP addresses in the same command, separated by spaces, or you can enter each command separately. The ASA tries each DNS server in order until it receives a response.

```
name-server ip_address [ip_address2] [...] [ip_address6]
```

Example:
```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```
Adjust ASP (Accelerated Security Path) Performance and Behavior

The ASP is an implementation layer that puts your policies and configurations into action. It is not of direct interest except during troubleshooting with the Cisco Technical Assistance Center. However, there are a few behaviors related to performance and reliability that you can adjust.

- Choose a Rule Engine Transactional Commit Model, page 14-15
- Enable ASP Load Balancing, page 14-16

Choose a Rule Engine Transactional Commit Model

By default, when you change a rule-based policy (such as access rules), the changes become effective immediately. However, this immediacy comes with a slight cost in performance. The performance cost is more noticeable for very large rule lists in a high connections-per-second environment, for example, when you change a policy with 25,000 rules while the ASA is handling 18,000 connections per second.

The performance is affected because the rule engine compiles rules to enable faster rule lookup. By default, the system also searches uncompiled rules when evaluating a connection attempt so that new rules can be applied; because the rules are not compiled, the search takes longer.

You can change this behavior so that the rule engine uses a transactional model when implementing rule changes, continuing to use the old rules until the new rules are compiled and ready for use. With the transactional model, performance should not drop during the rule compilation. The following table clarifies the behavioral difference.

<table>
<thead>
<tr>
<th>Model</th>
<th>Before Compilation</th>
<th>During Compilation</th>
<th>After Compilation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(The rate for connections per second decreases.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(The rate for connections per second is unaffected.)</td>
<td></td>
</tr>
</tbody>
</table>

An additional benefit of the transactional model is that, when replacing an ACL on an interface, there is no gap between deleting the old ACL and applying the new one. This feature reduces the chances that acceptable connections may be dropped during the operation.

Tip

If you enable the transactional model for a rule type, syslogs to mark the beginning and the end of the compilation are generated. These syslogs are numbered 780001 through 780004.

To enable the transactional commit model for the rule engine, use the following command:

```
asp rule-engine transactional-commit option
```

Where the options are:

- **access-group**—Access rules applied globally or to interfaces.
• nat—Network Address Translation rules.
Example:
ciscoasa(config)# asp rule-engine transactional-commit access-group

Enable ASP Load Balancing

The ASP load balancing mechanism helps avoid the following issues:
• Overruns caused by sporadic traffic spikes on flows
• Overruns caused by bulk flows oversubscribing specific interface receive rings
• Overruns caused by relatively heavily overloaded interface receive rings, in which a single core cannot sustain the load.

The asp load-balance per-packet command allows multiple cores to work simultaneously on packets that were received from a single interface receive ring. If the system drops packets, and the show cpu command output is far less than 100%, then this command may help your throughput if the packets belong to many unrelated connections. The auto option enables the ASA to automatically switch per-packet load balancing on and off.

To enable the automatic switching on and off of per-packet load balancing, enter the following command:
ciscoasa(config)# asp load-balance per-packet auto

Monitoring the DNS Cache

The ASA provides a local cache of DNS information from external DNS queries that are sent for certain clientless SSL VPN and certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache can not resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache with its corresponding hostname.

See the following command for monitoring the DNS cache:
• show dns-hosts

This command shows the DNS cache, which includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the name command.
## History for Basic Settings

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Passphrase</td>
<td>8.3(1)</td>
<td>We introduced this feature. The master passphrase allows you to securely store plain text passwords in encrypted format and provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. We introduced the following commands: key config-key password-encryption, password encryption aes, configure password encryption aes, show running-config password encryption aes, show password encryption.</td>
</tr>
<tr>
<td>Password Encryption Visibility</td>
<td>8.4(1)</td>
<td>We modified the <code>show password encryption</code> command.</td>
</tr>
<tr>
<td>Removal of the default Telnet password</td>
<td>9.0(2)/9.1(2)</td>
<td>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. The login password is only used for Telnet if you do not configure Telnet user authentication (the <code>aaa authentication telnet console</code> command). Previously, 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 <code>session</code> command). For initial ASASM access, you must use the <code>service-module session</code> command, until you set a login password. We modified the following command: <code>passwd</code>.</td>
</tr>
<tr>
<td>ASP Load Balancing</td>
<td>9.3(2)</td>
<td>We introduced this feature. The ASP load balancing mechanism reduces packet drop and improves throughput by allowing multiple cores of the CPU to receive packets from an interface receive ring and work on them independently. We introduced the following command: <code>asp load-balance per-packet-auto</code>.</td>
</tr>
</tbody>
</table>
Dynamic DNS

This chapter describes how to configure dynamic DNS (DDNS) update methods.

- About DDNS, page 15-1
- Guidelines for DDNS, page 15-2
- Configure DDNS, page 15-2
- Monitoring DDNS, page 15-7
- History for DDNS, page 15-7

About DDNS

DDNS update integrates DNS with DHCP. The two protocols are complementary: DHCP centralizes and automates IP address allocation; DDNS update automatically records the association between assigned addresses and hostnames at predefined intervals. DDNS allows frequently changing address-hostname associations to be updated frequently. Mobile hosts, for example, can then move freely on a network without user or administrator intervention. DDNS provides the necessary dynamic update and synchronization of the name-to-address mapping and address-to-name mapping on the DNS server.

The DDNS name and address mapping is held on the DHCP server in two resource records (RRs): the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method.

Related Topics

- Configure the DHCP Server, page 16-4

DDNS Update Configurations

The two most common DDNS update configurations are the following:

- The DHCP client updates the A RR, while the DHCP server updates the PTR RR.
- The DHCP server updates both the A RR and PTR RR.

In general, the DHCP server maintains DNS PTR RRs on behalf of clients. Clients may be configured to perform all desired DNS updates. The server may be configured to honor these updates or not. The DHCP server must know the fully qualified domain name (FQDN) of the client to update the PTR RR. The client provides an FQDN to the server using a DHCP option called Client FQDN.
UDP Packet Size

DDNS allows DNS requesters to advertise the size of their UDP packets and facilitates the transfer of packets larger than 512 octets. When a DNS server receives a request over UDP, it identifies the size of the UDP packet from the OPT RR and scales its response to contain as many resource records as are allowed in the maximum UDP packet size specified by the requester. The size of the DNS packets can be up to 4096 bytes for BIND or 1280 bytes for the Windows 2003 DNS Server. Several additional message-length maximum commands are available:

- The existing global limit: message-length maximum 512
- A client or server specific limit: message-length maximum client 4096 and message-length maximum server 4096
- The dynamic value specified in the OPT RR field: message-length maximum client auto

If the three commands are present at the same time, the ASA allows the automatically configured length up to the configured client or server maximum. For all other DNS traffic, the message-length maximum is used.

Guidelines for DDNS

This section includes guidelines and limitations that you should check before configuring DDNS.

Context Mode Guidelines

Supported in transparent firewall mode only for the DNS Client pane.

Configure DDNS

This section describes how to configure DDNS.

Update Both A and PTR RRs for Static IP Addresses

To configure the client to request that it update both A and PTR RRs for static IP addresses, perform the following steps:

Procedure

Step 1  Create a DDNS update method that dynamically updates DNS RRs.

```
  ddns update method name
```

Example:

```
ciscoasa(config)# ddns update method ddns-2
```

Step 2  Specify that the client update both the DNS A and PTR RRs.

```
  ddns both
```

Example:
Configure DDNS

Step 3 Configure an interface and enter interface configuration mode.

```
interface mapped_name
```

Example:
```
ciscoasa(DDNS-update-method)# interface eth1
```

Step 4 Associate the DDNS method with the interface and an update hostname.

```
ddns update [method-name | hostname hostname]
```

Example:
```
ciscoasa(config-if)# ddns update ddns-2
   ciscoasa(config-if)# ddns update hostname asa.example.com
```

Step 5 Configure a static IP address for the interface.

```
ip address ip_address [mask] [standby ip_address]
```

Example:
```
ciscoasa(config-if)# ip address 10.0.0.40 255.255.255.0
```

Update Both the A and PTR RRs

To configure the DHCP client to request that it update both the A and PTR RRs and that the DHCP server honor these requests, perform the following steps:

Procedure

Step 1 Configure the DHCP client to request that the DHCP server perform no updates.

```
dhcp-client update dns [server {both | none}]
```

Example:
```
ciscoasa(config)# dhcp-client update dns server none
```

Step 2 Create a DDNS update method that dynamically updates DNS RRs.

```
ddns update method name
```

Example:
```
ciscoasa(config)# ddns update method ddns-2
```

Step 3 Specify that the client update both the DNS A and PTR RRs.

```
ddns both
```

Example:
```
ciscoasa(DDNS-update-method)# ddns both
```

Step 4 Configure an interface and enter interface configuration mode.

```
interface mapped_name
```
Configure DDNS

Step 5  Associate the DDNS method with the interface and an update hostname.

```
ddns update [method-name | hostname hostname]
```

Example:
```
ciscoasa(config-if)# ddns update ddns-2
```
```
ciscoasa(config-if)# ddns update hostname asa.example.com
```

Step 6  Use DHCP to obtain an IP address for the interface.

```
ip address dhcp
```

Example:
```
ciscoasa(config-if)# ip address dhcp
```

Step 7  Configure the DHCP server to perform DDNS updates.

```
dhcpd update dns [both] [override] [interface srv_ifc_name]
```

Example:
```
ciscoasa(config-if)# dhcpd update dns
```

Ignore Updates to Either RR

To configure the DHCP client to include the FQDN option that instructs the DHCP server not to honor either the A or PTR updates, perform the following steps:

Procedure

Step 1  Create a DDNS update method that dynamically updates DNS RRs.

```
ddns update method name
```

Example:
```
ciscoasa(config)# ddns update method ddns-2
```

Step 2  Specify that the client updates both the DNS A and PTR RRs.

```
ddns both
```

Example:
```
ciscoasa(DDNS-update-method)# ddns both
```

Step 3  Configure an interface and enter interface configuration mode.

```
interface mapped_name
```

Example:
```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

Step 4  Associate the DDNS method with the interface and an update hostname.

```
ddns update [method-name | hostname hostname]
```

Example:
```
ciscoasa(DDNS-update-method)# interface Ethernet0
```
```
ciscoasa(DDNS-update-method)# ddns update ddns-2
```
```
ciscoasa(DDNS-update-method)# ddns update hostname asa.example.com
```

```
Configure DDNS

Example:
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com

**Step 5**  Configure the DHCP client to request that the DHCP server perform no updates.

dhcp-client update dns [server {both | none}]

Example:
ciscoasa(config)# dhcp-client update dns server none

**Step 6**  Use DHCP to obtain an IP address for the interface.

ip address dhcp

Example:
ciscoasa(if-config)# ip address dhcp

**Step 7**  Configure the DHCP server to override the client update requests.

dhcpd update dns [both | override] [interface srv_ifc_name]

Example:
ciscoasa(if-config)# dhcpd update dns both override

---

### Update the PTR RR Only

To configure the server to perform only PTR RR updates by default, perform the following steps:

**Procedure**

**Step 1**  Configure an interface.

interface mapped_name

Example:
ciscoasa(config)# interface Ethernet0

**Step 2**  Request that the DHCP server update both the DNS A and PTR RRs.

dhcp-client update dns [server {both | none}]

Example:
ciscoasa(config-if)# dhcp-client update dns both

**Step 3**  Configure the DHCP client on the configured interface.

ddns update [method-name | hostname hostname]

Example:
ciscoasa(config-if)# ddns update hostname asa

**Step 4**  Configure the DHCP server to perform DDNS updates.
Configure DDNS

```
dhcpd update dns [both] [override] [interface srv_ifc_name]
```

Example:
ciscoasa(config-if)# dhcpd update dns

### Step 5
Define the DNS domain name for DHCP clients.
```
dhcpd domain domain_name [interface if_name]
```

Example:
ciscoasa(config-if)# dhcpd domain example.com

---

**Update a RR with the Client and a PTR RR with the Server**

To configure the client to update the A resource record and to configure the server to update the PTR records, perform the following steps:

**Procedure**

1. **Step 1** Create a DDNS update method that dynamically updates DNS RRs.
   ```
   ddns update method name
   ```
   Example:
ciscoasa(config)# ddns update method ddns-2

2. **Step 2** Specify a DDNS update method.
   ```
   ddns both
   ```
   Example:
ciscoasa(DDNS-update-method)# ddns both

3. **Step 3** Configure an interface.
   ```
   interface mapped_name
   ```
   Example:
ciscoasa(DDNS-update-method)# interface Ethernet0

4. **Step 4** Configure the update parameters that the DHCP client passes to the DHCP server.
   ```
   dhcp-client update dns [server {both | none}]
   ```
   Example:
ciscoasa(config-if)# dhcp-client update dns

5. **Step 5** Associate the DDNS method with the interface and an update hostname.
   ```
   ddns update [method-name | hostname hostname]
   ```
   Example:
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa
Step 6 Configure the DHCP server to perform DDNS updates.

```
dhcpd update dns [both] [override] [interface srv_ifc_name]
```

Example:

```
ciscoasa(if-config)# dhcpd update dns
```

Step 7 Define the DNS domain name for DHCP clients.

```
dhcpd domain domain_name [interface if_name]
```

Example:

```
ciscoasa(config-if)# dhcpd domain example.com
```

Monitoring DDNS

See the following commands for monitoring DDNS status:

- **show running-config ddns**
  
  This command shows the current DDNS configuration.

- **show running-config dns server-group**
  
  This command shows the current DNS server group status.

History for DDNS

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDNS</td>
<td>7.0(1)</td>
<td>We introduced this feature. We introduced the following commands: <code>ddns</code>, <code>ddns update</code>, <code>dhcp client update dns</code>, <code>dhcpd update dns</code>, <code>show running-config ddns</code>, and <code>show running-config dns server-group</code>.</td>
</tr>
</tbody>
</table>
DHCP Services

This chapter describes how to configure the DHCP server or DHCP relay.

- About the DHCP Server, page 16-1
- About the DHCP Relay Agent, page 16-2
- Licensing Requirements for DHCP Services, page 16-2
- Guidelines for DHCP Services, page 16-2
- Configure the DHCP Server, page 16-4
- Monitoring DHCP Services, page 16-11
- History for DHCP Services, page 16-12

About the DHCP Server

DHCP provides network configuration parameters, such as IP addresses, to DHCP clients. The Cisco ASA can provide a DHCP server to DHCP clients attached to ASA interfaces. The DHCP server provides network configuration parameters directly to DHCP clients.

A client locates a DHCP server to request the assignment of configuration information using a reserved, link-scoped multicast address, which indicates that the client and server should be attached to the same link. However, in some cases where ease of management, economy, or scalability is the concern, we recommend that you allow a DHCP client to send a message to a server that is not connected to the same link. The DHCP relay agent, which may reside on the client network, can relay messages between the client and server. The relay agent operation is transparent to the client.

An IPv4 DHCP client uses a broadcast rather than a multicast address to reach the server. The DHCP client listens for messages on UDP port 68; the DHCP server listens for messages on UDP port 67.

DHCP for IPv6 (DHCPv6) specified in RFC 3315 enables IPv6 DHCP servers to send configuration parameters such as network addresses or prefixes and DNS server addresses to IPv6 nodes (that is, DHCP clients). DHCPv6 uses the following multicast addresses:

- All_DHCP_Relay_Agents_and_Servers (FF02::1:2) is a link-scoped multicast address used by a client to communicate with neighboring (that is, on-link) relay agents and servers. All DHCPv6 servers and relay agents are members of this multicast group.
- The DHCPv6 relay service and server listen for messages on UDP port 547. The ASA DHCPv6 relay agent listens on both UDP port 547 and the All_DHCP_Relay_Agents_and_Servers multicast address.
About the DHCP Relay Agent

You can configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers. DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the ASA because it does not forward broadcast traffic.

You can remedy this situation by configuring the interface of your ASA that is receiving the broadcasts to forward DHCP requests to a DHCP server on another interface.

Licensing Requirements for DHCP Services

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA v</td>
<td>Standard or Premium License.</td>
</tr>
<tr>
<td>All other models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>

For all ASA models, the maximum number of DHCP client addresses varies depending on the license:
- If the limit is 10 hosts, the maximum available DHCP pool is 32 addresses.
- If the limit is 50 hosts, the maximum available DHCP pool is 128 addresses.
- If the number of hosts is unlimited, the maximum available DHCP pool is 256 addresses.

Guidelines for DHCP Services

This section describes guidelines and limitations that you should check before configuring DHCP services.

Firewall Mode Guidelines

DHCP server is supported in transparent firewall mode.
DHCP relay is NOT supported in transparent firewall mode.

IPv6 Guidelines

Does not support IPv6 for interface-specific DHCP relay servers.

DHCP Server Guidelines

- The maximum available DHCP pool is 256 addresses.
- You can configure only one DHCP server on each interface of the ASA. Each interface can have its own pool of addresses to use. However the other DHCP settings, such as DNS servers, domain name, options, ping timeout, and WINS servers, are configured globally and used by the DHCP server on all interfaces.
- You cannot configure a DHCP client or DHCP relay service on an interface on which the server is enabled. Additionally, DHCP clients must be directly connected to the interface on which the server is enabled.
Guidelines for DHCP Services

- The ASA does not support QIP DHCP servers for use with the DHCP proxy service.
- The relay agent cannot be enabled if the DHCP server is also enabled.
- The ASA DHCP server does not support BOOTP requests. In multiple context mode, you cannot enable the DHCP server or DHCP relay service on an interface that is used by more than one context.
- When it receives a DHCP request, the ASA sends a discovery message to the DHCP server. This message includes the IP address (within a subnetwork) that was configured with the `dhcp-network-scope` command in the group policy. If the server has an address pool that falls within that subnetwork, the server sends the offer message with the pool information to the IP address—not to the source IP address of the discovery message.
- When a client connects, the ASA sends a discovery message to all the servers in the server list. This message includes the IP address (within a subnetwork) that was configured with the `dhcp-network-scope` command in the group policy. The ASA selects the first offer received and drops the other offers. If the server has an address pool that falls within that subnetwork, the server sends the offer message with the pool information to the IP address—not to the source IP address of the discovery message. When the address needs to be renewed, it attempts to renew it with the lease server (the server from which the address was acquired). If the DHCP renew fails after a specified number of retries (four attempts), the ASA moves to the DHCP rebind phase after a predefined time period. During the rebind phase, the ASA simultaneously sends requests to all servers in the group. In a high availability environment, lease information is shared, so the other servers can acknowledge the lease and ASA will return to the bound state. During the rebind phase, if there is no response from any of the servers in the server list (after three retries), then the ASA will purge the entries.

For example, if the server has a pool in the range of 209.165.200.225 to 209.165.200.254, mask 255.255.255.0, and the IP address specified by the `dhcp-network-scope` command is 209.165.200.1, the server sends that pool in the offer message to the ASA.

The `dhcp-network-scope` command setting applies only to VPN users.

DHCP Relay Guidelines

- You can configure a maximum of 10 DHCPv4 relay servers in single mode and per context, global and interface-specific servers combined, with a maximum of 4 servers per interface.
- You can configure a maximum of 10 DHCPv6 relay servers in single mode and per context. Interface-specific servers for IPv6 are not supported.
- The relay agent cannot be enabled if the DHCP server feature is also enabled.
- When the DHCP relay service is enabled and more than one DHCP relay server is defined, the ASA forwards client requests to each defined DHCP relay server. Replies from the servers are also forwarded to the client until the client DHCP relay binding is removed. The binding is removed when the ASA receives any of the following DHCP messages: ACK, NACK, ICMP unreachable, or decline.
- You cannot enable DHCP relay service on an interface running as a DHCP proxy service. You must remove the VPN DHCP configuration first or an error message appears. This error occurs if both DHCP relay and DHCP proxy services are enabled. Make sure that either the DHCP relay or DHCP proxy service is enabled, but not both.
- DHCP relay services are not available in transparent firewall mode. You can, however, allow DHCP traffic through using an access list. To allow DHCP requests and replies through the ASA in transparent mode, you need to configure two access lists, one that allows DHCP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.
- For IPv4, clients must be directly-connected to the ASA and cannot send requests through another relay agent or a router. For IPv6, the ASA supports packets from another relay server.
Configure the DHCP Server

This section describes how to configure a DHCP server provided by the ASA.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Enable the DHCP Server. See Enable the DHCP Server, page 16-4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Configure either a DHCPv4 relay agent or a DHCPv6 relay agent. See Configure the DHCPv4 Relay Agent, page 16-9 or Configure the DHCPv6 Relay Agent, page 16-11.</td>
</tr>
</tbody>
</table>

Enable the DHCP Server

To enable the DHCP server on an ASA interface, perform the following steps:

Procedure

Step 1  Create a DHCP address pool. The ASA assigns a client one of the addresses from this pool to use for a given period of time. These addresses are the local, untranslanted addresses for the directly connected network.

```
dhcpd address ip_address if_name
```

Example:

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

The address pool must be on the same subnet as the ASA interface.

Step 2  (Optional) Specify the IP address(es) of the DNS server(s).

```
dhcpd dns dns1 [dns2]
```

Example:

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

Step 3  (Optional) Specify the IP address(es) of the WINS server(s). You may specify up to two WINS servers.

```
dhcpd wins wins1 [wins2]
```
Configure the DHCP Server

Example:
```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

**Step 4**  
(Optional) Change the lease length to be granted to the client. The lease length equals the amount of time in seconds that the client can use its allocated IP address before the lease expires. Enter a value from 0 to 1,048,575. The default value is 3600 seconds.

```
dhcpd lease lease_length
```

Example:
```
ciscoasa(config)# dhcpd lease 3000
```

**Step 5**  
(Optional) Configure the domain name.

```
dhcpd domain domain_name
```

Example:
```
ciscoasa(config)# dhcpd domain example.com
```

**Step 6**  
(Optional) Configure the DHCP ping timeout value for ICMP packets. To avoid address conflicts, the ASA sends two ICMP ping packets to an address before assigning that address to a DHCP client.

```
dhcpd ping_timeout milliseconds
```

Example:
```
ciscoasa(config)# dhcpd ping timeout 20
```

**Step 7**  
Define a default gateway that is sent to DHCP clients. If you do not use the **dhcpd option 3** command to define the default gateway, DHCP clients use the ASA interface IP address that is closest to the DHCP clients by default; the ASA does not use the management interface IP address. As a result, the DHCP ACK does not include this option.

```
dhcpd option 3 ip gateway_ip
```

Example:
```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

**Step 8**  
Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface.

```
dhcpd enable interface_name
```

Example:
```
ciscoasa(config)# dhcpd enable outside
```
Configure Advanced DHCP Options

The ASA supports the DHCP options listed in RFC 2132, RFC 2562, and RFC 5510 to send information. You can use advanced DHCP options to provide DNS, WINS, and domain name parameters to DHCP clients. You can also use the DHCP automatic configuration setting to obtain these values or define them manually. When you use more than one method to define this information, it is passed to DHCP clients in the following sequence:

1. Manually configured settings.
2. Advanced DHCP options settings.
3. DHCP automatic configuration settings.

For example, you can manually define the domain name that you want the DHCP clients to receive and then enable DHCP automatic configuration. Although DHCP automatic configuration discovers the domain together with the DNS and WINS servers, the manually defined domain name is passed to DHCP clients with the discovered DNS and WINS server names, because the domain name discovered by the DHCP automatic configuration process is superseded by the manually defined domain name.

Return an IP Address

To configure an DHCP option that returns one or two IP addresses, perform the following steps:

Procedure

Step 1 Configure a DHCP option that returns one or two IP addresses.

```
dhcpd option code ip addr_1 [addr_2]
```

Example:
```
ciscoasa(config)# dhcpd option 2 ip 10.10.1.1 10.10.1.2
```

Return a Text String

To configure an DHCP option that returns a text string, perform the following steps:

Procedure

Step 1 Configure a DHCP option that returns a text string.

```
dhcpd option code ascii text
```

Example:
```
ciscoasa(config)# dhcpd option 2 ascii examplestring
```
Return a Hexadecimal Value

To configure an DHCP option that returns a hexadecimal value, perform the following steps:

Procedure

Step 1
Configure a DHCP option that returns a hexadecimal value.

dhcpd option code hex value

Example:
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11

The ASA does not verify that the option type and value that you provide match the expected type and value for the option code as defined in RFC 2132. For example, you can enter the dhcpd option 46 ascii hello command, and the ASA accepts the configuration, although option 46 is defined in RFC 2132 to expect a single-digit, hexadecimal value. For more information about option codes and their associated types and expected values, see RFC 2132.

Table 16-1 shows the DHCP options that are not supported by the dhcpd option command.

<table>
<thead>
<tr>
<th>Option Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>DHCPOPT_PAD</td>
</tr>
<tr>
<td>1</td>
<td>HCPOPT_SUBNET_MASK</td>
</tr>
<tr>
<td>12</td>
<td>DHCPOPT_HOST_NAME</td>
</tr>
<tr>
<td>50</td>
<td>DHCPOPT_REQUESTED_ADDRESS</td>
</tr>
<tr>
<td>51</td>
<td>DHCPOPT_LEASE_TIME</td>
</tr>
<tr>
<td>52</td>
<td>DHCPOPT_OPTION_OVERLOAD</td>
</tr>
<tr>
<td>53</td>
<td>DHCPOPT_MESSAGE_TYPE</td>
</tr>
<tr>
<td>54</td>
<td>DHCPOPT_SERVER_IDENTIFIER</td>
</tr>
<tr>
<td>58</td>
<td>DHCPOPT_RENEWAL_TIME</td>
</tr>
<tr>
<td>59</td>
<td>DHCPOPT_REBINDING_TIME</td>
</tr>
<tr>
<td>61</td>
<td>DHCPOPT_CLIENT_IDENTIFIER</td>
</tr>
<tr>
<td>67</td>
<td>DHCPOPT_BOOT_FILE_NAME</td>
</tr>
<tr>
<td>82</td>
<td>DHCPOPT_RELAY_INFORMATION</td>
</tr>
<tr>
<td>255</td>
<td>DHCPOPT_END</td>
</tr>
</tbody>
</table>

DHCP options 3, 66, and 150 are used to configure Cisco IP phones. For more information about configuring these options, see Configure Cisco IP Phones with a DHCP Server, page 16-8.
Configure Cisco IP Phones with a DHCP Server

Cisco IP phones download their configuration from a TFTP server. When a Cisco IP phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

- DHCP option 150 provides the IP addresses of a list of TFTP servers.
- DHCP option 66 gives the IP address or the hostname of a single TFTP server.

Note: Cisco IP phones can also include DHCP option 3 in their requests, which sets the default route.

A single request might include both options 150 and 66. In this case, the ASA DHCP server provides values for both options in the response if they are already configured on the ASA.

Any Option Number

To send information to use for any option number, perform the following steps:

Procedure

Step 1: Provide information for DHCP requests that include an option number as specified in RFC 2132.

```bash
dhcpd option number value
```

Example:
```
ciscoasa(config)# dhcpd option 2
```

Option 66

To send information to use for option 66, perform the following steps:

Procedure

Step 1: Provide the IP address or name of a TFTP server for option 66.

```bash
dhcpd option 66 ascii server_name
```

Example:
```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

Option 150

To send information to use for option 150, perform the following steps:

Procedure

Step 1: Provide the IP address or names of one or two TFTP servers for option 150.
Configure the DHCP Server

dhcpd option 150 ip server_ip1 [server_ip2]

Example:
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1

The server_ip1 is the IP address or name of the primary TFTP server while server_ip2 is the IP address or name of the secondary TFTP server. A maximum of two TFTP servers can be identified using option 150.

Option 3

To send information to use for option 3, perform the following steps:

Procedure

Step 1 Set the default route.
dhcpd option 3 ip router_ip1

Example:
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1

Configure the DHCPv4 Relay Agent

When a DHCP request enters an interface, the DHCP servers to which the ASA relays the request depends on your configuration. You may configure the following types of servers:

- Interface-specific DHCP servers—When a DHCP request enters a particular interface, then the ASA relays the request only to the interface-specific servers.
- Global DHCP servers—When a DHCP request enters an interface that does not have interface-specific servers configured, the ASA relays the request to all global servers. If the interface has interface-specific servers, then the global servers are not used.

Procedure

Step 1 Do one or both of the following:

- Specify a global DHCP server IP address and the interface through which it is reachable.
  dhcprelay server ip_address if_name

  Example:
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it

- Specify the interface ID connected to the DHCP client network, and the DHCP server IP address to be used for DHCP requests that enter that interface.

  interface interface_id
dhcprelay server ip_address
Configure the DHCP Server

Example:
```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

Note that you do not specify the egress interface for the requests, as in the global `dhcprelay server` command; instead, the ASA uses the routing table to determine the egress interface.

**Step 2** Enable the DHCP relay service on the interface connected to the DHCP clients. You may enable DHCP relay on multiple interfaces.
```
dhcprelay enable interface
```

Example:
```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

**Step 3** (Optional) Set the number of seconds allowed for DHCP relay address handling.
```
dhcprelay timeout seconds
```

Example:
```
ciscoasa(config)# dhcprelay timeout 25
```

**Step 4** (Optional) Change the first default router address in the packet sent from the DHCP server to the address of the ASA interface.
```
dhcprelay setroute interface_name
```

Example:
```
ciscoasa(config)# dhcprelay setroute inside
```

This action allows the client to set its default route to point to the ASA even if the DHCP server specifies a different router.

If there is no default router option in the packet, the ASA adds one containing the interface address.

**Step 5** (Optional) Do one of the following:

- Specify a DHCP client interface that you want to trust.

```
interface interface_id
dhcprelay information trusted
```

Example:
```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# dhcprelay information trusted
```

You can 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.
Configure all client interfaces as trusted.

dhcprelay information trust-all

Example:
ciscoasa(config)# dhcprelay information trust-all

Configure the DHCPv6 Relay Agent

When a DHCPv6 request enters an interface, then the ASA relays the request to all DHCPv6 global servers.

Procedure

Step 1 Specify the IPv6 DHCP server destination address to which client messages are forwarded.

ipv6 dhcprelay server ipv6_address [interface]

Example:
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701

The ipv6-address argument can be a link-scoped unicast, multicast, site-scoped unicast, or global IPv6 address. Unspecified, loopback, and node-local multicast addresses are not allowed as the relay destination. The optional interface argument specifies the egress interface for a destination. Client messages are forwarded to the destination address through the link to which the egress interface is connected. If the specified address is a link-scoped address, then you must specify the interface.

Step 2 Enable DHCPv6 relay service on a client interface.

ipv6 dhcprelay enable interface

Example:
ciscoasa(config)# ipv6 dhcprelay enable inside

Step 3 (Optional) Specify the amount of time in seconds that is allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding for relay address handling.

ipv6 dhcprelay timeout seconds

Example:
ciscoasa(config)# ipv6 dhcprelay timeout 25

Valid values for the seconds argument range from 1 to 3600. The default is 60 seconds.

Monitoring DHCP Services

See the following commands for monitoring DHCP services:

- show running-config dhcpd

  This command shows the current DHCP configuration.
History for DHCP Services

Table 16-2  History for DHCP Services

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>7.0(1)</td>
<td>The ASA can provide a DHCP server or DHCP relay services to DHCP clients attached to ASA interfaces. We introduced the following commands: dhcp client update dns, dhcpd address, dhcpd domain, dhcpd enable, dhcpd lease, dhcpd option, dhcpd ping timeout, dhcpd update dns, dhcpd wins, dhcp-network-scope, dhcprelay enable, dhcprelay server, dhcprelay setroute, dhcp-server, show running-config dhcpd, and show running-config dhcprelay.</td>
</tr>
<tr>
<td>DHCP for IPv6 (DHCPv6)</td>
<td>9.0(1)</td>
<td>Support for IPv6 was added. We introduced the following commands: ipv6 dhcprelay server, ipv6 dhcprelay enable, ipv6 dhcprelay timeout, clear config ipv6 dhcprelay, ipv6 nd managed-config-flag, ipv6 nd other-config-flag, debug ipv6 dhcp, debug ipv6 dhcprelay, show ipv6 dhcprelay binding, clear ipv6 dhcprelay binding, show ipv6 dhcprelay statistics, and clear ipv6 dhcprelay statistics.</td>
</tr>
<tr>
<td>DHCP relay servers per interface (IPv4 only)</td>
<td>9.1(2)</td>
<td>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. We introduced or modified the following commands: dhcprelay server (interface config mode), clear configure dhcprelay, show running-config dhcprelay.</td>
</tr>
</tbody>
</table>
DHCP trusted interfaces

9.1(2) 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.

We introduced or modified the following commands: `dhcprelay information trusted`, `dhcprelay information trust-all`, `show running-config dhcprelay`.

DHCP rebind function

9.1(4) During the DHCP rebind phase, the client now tries to rebind to other DHCP servers in the tunnel group list. Before this release, the client did not rebind to an alternate server when the DHCP lease fails to renew.

We did not introduce or modify any commands.
PART 5

Objects and ACLs
Objects for Access Control

Objects are reusable components for use in your configuration. You can define and use them in Cisco ASA configurations in the place of inline IP addresses, services, names, and so on. Objects make it easy to maintain your configurations because you can modify an object in one place and have it be reflected in all other places that are referencing it. Without objects you would have to modify the parameters for every feature when required, instead of just once. For example, if a network object defines an IP address and subnet mask, and you want to change the address, you only need to change it in the object definition, not in every feature that refers to that IP address.

- Guidelines for Objects, page 17-1
- Configure Objects, page 17-2
- Monitoring Objects, page 17-10
- History for Objects, page 17-11

Guidelines for Objects

IPv6 Guidelines

Supports IPv6 with the following restrictions:

- The ASA does not support IPv6 nested network object groups, so you cannot group an object with IPv6 entries under another IPv6 object group.
- You can mix IPv4 and IPv6 entries in a network object group; you cannot use a mixed object group for NAT.

Additional Guidelines and Limitations

- Objects must have unique names, because objects and object groups share the same name space. While you might want to create a network object group named “Engineering” and a service object group named “Engineering,” you need to add an identifier (or “tag”) to the end of at least one object group name to make it unique. For example, you can use the names “Engineering_admins” and “Engineering_hosts” to make the object group names unique and to aid in identification.
- Object names are limited to 64 characters, including letters, numbers, and these characters: .!@#$%^&()-_. Object names are case-sensitive.
- You cannot remove an object or make an object empty if it is used in a command, unless you enable forward referencing (the forward-reference enable command).
Configure Objects

The following sections describe how to configure objects that are primarily used on access control.

- Configure Network Objects and Groups, page 17-2
- Configure Service Objects and Service Groups, page 17-4
- Configure Local User Groups, page 17-7
- Configure Security Group Object Groups, page 17-8
- Configure Time Ranges, page 17-9

Configure Network Objects and Groups

Network objects and groups identify IP addresses or host names. Use these objects in access control lists to simplify your rules.

- Configure a Network Object, page 17-2
- Configure a Network Object Group, page 17-3

Configure a Network Object

A network object can contain a host, a network IP address, a range of IP addresses, or a fully qualified domain name (FQDN).

You can also enable NAT rules on the object (excepting FQDN objects). See the firewall configuration guide for more information about configuring object NAT.

Procedure

Step 1
Create or edit a network object using the object name.

ciscoasa(config)# object network object_name

Example

ciscoasa(config)# object network email-server

Step 2
Add an address to the object using one of the following commands. Use the no form of the command to remove the object.

- **host** *(IPv4_address | IPv6_address)*—The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.

- **subnet** *(IPv4_address IPv4_mask | IPv6_address/IPv6_prefix)*—The address of a network. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.

- **range** *(start_address end_address)*—A range of addresses. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes.

- **fqdn** *(v4 | v6)* *(fully_qualified_domain_name)*—A fully-qualified domain name, that is, the name of a host, such as www.example.com. Specify v4 to limit the address to IPv4, and v6 for IPv6. If you do not specify an address type, IPv4 is assumed.

Example
Configure Objects

Step 3 (Optional) Add a description.
ciscoasa(config-network-object)# description string

Configure a Network Object Group

Network object groups can contain multiple network objects as well as inline networks or hosts. Network object groups can include a mix of both IPv4 and IPv6 addresses.

However, you cannot use a mixed IPv4 and IPv6 object group for NAT, or object groups that include FQDN objects.

Procedure

Step 1 Create or edit a network object group using the object name.
ciscoasa(config)# object-group network group_name

Example

ciscoasa(config)# object-group network admin

Step 2 Add objects and addresses to the network object group using one or more of the following commands. Use the no form of the command to remove an object.

- network-object host {IPv4_address | IPv6_address}—The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.
- network-object {IPv4_address | IPv6_address | IPv4_mask | IPv6_address/IPv6_prefix}—The address of a network or host. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.
- network-object object object_name—The name of an existing network object.
- group-object object_group_name—The name of an existing network object group.

Example

ciscoasa(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
ciscoasa(config-network-object-group)# network-object 2001:DB8::0DB8:800:200C:417A
ciscoasa(config-network-object-group)# group-object existing-network-object-group

Step 3 (Optional) Add a description.
ciscoasa(config-network-object-group)# description string

Example

To create a network group that includes the IP addresses of three administrators, enter the following commands:

hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
Configure Objects

Create network object groups for privileged users from various departments by entering the following commands:

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89
hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12
hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

You then nest all three groups together as follows:

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

Configure Service Objects and Service Groups

Service objects and groups identify protocols and ports. Use these objects in access control lists to simplify your rules.

- Configure a Service Object, page 17-4
- Configure a Service Group, page 17-5

Configure a Service Object

A service object can contain a single protocol, ICMP, ICMPv6, TCP or UDP port or port ranges.

**Procedure**

**Step 1** Create or edit a service object using the object name.

```
ciscoasa(config)# object service object_name
```

Example

```
ciscoasa(config)# object service web
```

**Step 2** Add a service to the object using one of the following commands. Use the **no** form of the command to remove an object.

- **service protocol**—The name or number (0-255) of an IP protocol. Specify **ip** to apply to all protocols. For a list of supported keywords, see Protocols and Applications, page 43-10.
**Configure Objects**

- **service [icmp | icmp6] [icmp-type [icmp_code]]**—For ICMP or ICMP version 6 messages. You can optionally specify the ICMP type by name or number (0-255) to limit the object to that message type. If you specify a type, you can optionally specify an ICMP code for that type (1-255). If you do not specify the code, then all codes are used. For a list of ICMP types, see ICMP Types, page 43-15.

- **service [tcp | udp] [source operator port] [destination operator port]**—For TCP or UDP. You can optionally specify ports for the source, destination, or both. You can specify the port by name or number (for a list, see TCP and UDP Ports, page 43-11). The operator can be one of the following:
  - **lt**—less than.
  - **gt**—greater than.
  - **eq**—equal to.
  - **neq**—not equal to.
  - **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example, range 100 200.

Example

```
ciscoasa(config-service-object)# service tcp destination eq http
```

**Step 3** (Optional) Add a description.

```
ciscoasa(config-service-object)# description string
```

---

**Configure a Service Group**

A service object group includes a mix of protocols, if desired, including optional source and destination ports for TCP or UDP.

**Before You Begin**

You can model all services using the generic service object group, which is explained here. However, you can still configure the types of service group objects that were available prior to ASA 8.3(1). These legacy objects include TCP/UDP/TCP-UDP port groups, protocol groups, and ICMP groups. The contents of these groups are equivalent to the associated configuration in the generic service object group, with the exception of ICMP groups, which do not support ICMP6 or ICMP codes. If you still want to use these legacy objects, for detailed instructions, see the `object-service` command description in the command reference on Cisco.com.

**Procedure**

**Step 1** Create or edit a service object group using the object name.

```
ciscoasa(config)# object-group service group_name
```

Example

```
ciscoasa(config)# object-group service general-services
```

**Step 2** Add objects and services to the service object group using one or more of the following commands. Use the **no** form of the command to remove an object.

- **service-object protocol**—The name or number (0-255) of an IP protocol. Specify **ip** to apply to all protocols. For a list of supported keywords, see Protocols and Applications, page 43-10.
Configure Objects

- **service-object {icmp | icmp6} [icmp-type [icmp_code]]** — For ICMP or ICMP version 6 messages. You can optionally specify the ICMP type by name or number (0-255) to limit the object to that message type. If you specify a type, you can optionally specify an ICMP code for that type (1-255). If you do not specify the code, then all codes are used. For a list of ICMP types, see ICMP Types, page 43-15.

- **service-object {tcp | udp | tcp-udp} [source operator port] [destination operator port]** — For TCP, UDP, or both. You can optionally specify ports for the source, destination, or both. You can specify the port by name or number (for a list, see TCP and UDP Ports, page 43-11). The operator can be one of the following:
  - `lt` — less than.
  - `gt` — greater than.
  - `eq` — equal to.
  - `neq` — not equal to.
  - `range` — an inclusive range of values. When you use this operator, specify two port numbers, for example, `range 100 200`.

- **service-object object object_name** — The name of an existing service object.

- **group-object object_group_name** — The name of an existing service object group.

Example

```
ciscoasa(config-service-object-group)# service-object ipsec
```

```
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
```

```
ciscoasa(config-service-object-group)# service-object icmp echo
```

```
ciscoasa(config-service-object-group)# service-object object my-service
```

```
ciscoasa(config-service-object-group)# group-object Engineering_groups
```

**Step 3** (Optional) Add a description.

```
ciscoasa(config-service-object-group)# description string
```

**Examples**

The following example shows how to add both TCP and UDP services to a service object group:

```
ciscoasa(config)# object-group service CommonApps
```

```
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
```

```
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
```

```
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
```

```
ciscoasa(config-service-object-group)# service-object tcp destination eq https
```

```
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

The following example shows how to add multiple service objects to a service object group:

```
ciscoasa(config)# object service SSH
```

```
ciscoasa(config-service-object)# service tcp destination eq ssh
```

```
ciscoasa(config)# object service EIGRP
```

```
ciscoasa(config-service-object)# service eigrp
```

```
ciscoasa(config)# object service HTTPS
```

```
ciscoasa(config-service-object)# service tcp source range 1 1024 destination eq https
```

```
ciscoasa(config)# object-group service Group1
```

```
ciscoasa(config-service-object-group)# service-object object SSH
```

```
ciscoasa(config-service-object-group)# service-object object EIGRP
```

```
ciscoasa(config-service-object-group)# service-object object HTTPS
```

```
ciscoasa(config-service-object-group)# service-object object HTTPS
```
Configure Local User Groups

You can create local user groups for use in features that support the identity firewall by including the group in an extended ACL, which in turn can be used in an access rule, for example.

The ASA sends an LDAP query to the Active Directory server for user groups globally defined in the Active Directory domain controller. The ASA imports these groups for identity-based rules. However, the ASA might have localized network resources that are not defined globally that require local user groups with localized security policies. Local user groups can contain nested groups and user groups that are imported from Active Directory. The ASA consolidates local and Active Directory groups.

A user can belong to local user groups and user groups imported from Active Directory.

Because you can use usernames and user group names directly in an ACL, you need to configure local user groups only if:

- You want to create a group of users defined in the LOCAL database.
- You want to create a group of users or user groups that are not captured in a single user group defined on the AD server.

For information on how to enable the identity firewall, see Chapter 32, “Identity Firewall.”

Procedure

Step 1
Create or edit a user object group using the object name.

```plaintext
CiscoASA(config)# object-group user group_name
```

Example

```plaintext
CiscoASA(config)# object-group user admins
```

Step 2
Add users and groups to the user object group using one or more of the following commands. Use the no form of the command to remove an object.

- `user [domain_NETBIOS_name\]username`—A username. If there is a space in the domain name or username, you must enclose the domain name and user name in quotation marks. The domain name can be LOCAL (for users defined in the local database) or an Active Directory (AD) domain name as specified in the `user-identity domain domain_NetBIOS_name aaa-server` `aaa_server_group_tag` command. When adding users defined in an AD domain, the `user_name` must be the Active Directory sAMAccountName, which is unique, instead of the common name (cn), which might not be unique. If you do not specify a domain name, the default is used, which is either LOCAL or the one defined on the `user-identity default-domain` command.

- `user-group [domain_NETBIOS_name\]username`—A user group. If there is a space in the domain name or group name, you must enclose the domain name and group name in quotation marks. Note the double \ that separates the domain and group names.

- `group-object object_group_name`—The name of an existing user object group.

Example

```plaintext
CiscoASA(config-user-object-group)# user EXAMPLE\admin
CiscoASA(config-user-object-group)# user-group EXAMPLE\managers
CiscoASA(config-user-object-group)# group-object local-admins
```

Step 3
(Optional) Add a description.

```plaintext
CiscoASA(config-user-object-group)# description string
```
Configure Security Group Object Groups

You can create security group object groups for use in features that support Cisco TrustSec by including the group in an extended ACL, which in turn can be used in an access rule, for example.

When integrated with Cisco TrustSec, the ASA downloads security group information from the ISE. The ISE acts as an identity repository, by providing Cisco TrustSec tag-to-user identity mapping and Cisco TrustSec tag-to-server resource mapping. You provision and manage security group ACLs centrally on the ISE.

However, the ASA might have localized network resources that are not defined globally that require local security groups with localized security policies. Local security groups can contain nested security groups that are downloaded from the ISE. The ASA consolidates local and central security groups.

To create local security groups on the ASA, you create a local security object group. A local security object group can contain one or more nested security object groups or Security IDs or security group names. You can also create a new Security ID or security group name that does not exist on the ASA.

You can use the security object groups you create on the ASA to control access to network resources. You can use the security object group as part of an access group or service policy.

For information on how to integrate the ASA with TrustSec, see Chapter 33, “ASA and Cisco TrustSec.”

Tip

If you create a group with tags or names that are not known to the ASA, any rules that use the group will be inactive until the tags or names are resolved with ISE.

Procedure

Step 1

Create or edit a security group object group using the object name.

ciscoasa(config)# object-group security group_name

Example

ciscoasa(config)# object-group security mktg-sg

Step 2

Add objects to the service group object group using one or more of the following commands. Use the no form of the command to remove an object.

- **security-group** (tag sgt_number | name sg_name)—A security group tag (SGT) or name. A tag is a number from 1 to 65533 and is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB) by the ISE. Security group names are created on the ISE and provide user-friendly names for security groups. The security group table maps SGTs to security group names. Consult your ISE configuration for the valid tags and names.

- **group-object** object_group_name—The name of an existing security group object group.

Example

```bash
ciscoasa(config-security-object-group)# security-group tag 1
```  
```bash
ciscoasa(config-security-object-group)# security-group name mgkt
```  
```bash
ciscoasa(config-security-object-group)# group-object local-sg
```  

Step 3

(Optional) Add a description.
Configure Time Ranges

A time range object defines a specific time consisting of a start time, an end time, and optional recurring entries. You use these objects on ACL rules to provide time-based access to certain features or assets. For example, you could create an access rule that allows access to a particular server during working hours only.

Note

You can include multiple periodic entries in a time range object. If a time range has both absolute and periodic values specified, then the periodic values are evaluated only after the absolute start time is reached, and they are not further evaluated after the absolute end time is reached.

Creating a time range does not restrict access to the device. This procedure defines the time range only. You must then use the object in an access control rule.

Procedure

Step 1

Create the time range.

ciscoasa(config-security-object-group)# time-range name

Step 2

(Optional.) Add a start or end time (or both) to the time range.

```ciscoasa(config-security-object-group)# absolute [start time date] [end time date]
```

If you do not specify a start time, the default start time is now.

The time is in the 24-hour format `hh:mm`. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

The date is in the format `day month year`; for example, 1 January 2014.

Step 3

(Optional.) Add recurring time periods.

```ciscoasa(config-security-object-group)# periodic days-of-the-week time to [days-of-the-week] time
```

You can specify the following values for `days-of-the-week`. Note that you can specify a second day of the week only if you specify a single day for the first argument.

- `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`, or `Sunday`. You can specify more than one of these, separated by spaces, for the first `days-of-the-week` argument.
- `daily`
- `weekdays`
- `weekend`

The time is in the 24-hour format `hh:mm`. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

You can repeat this command to configure more than one recurring period.
Examples
The following is an example of an absolute time range beginning at 8:00 a.m. on January 1, 2006. Because no end time and date are specified, the time range is in effect indefinitely.
\[
ciscoasa(config)# time-range for2006
ciscoasa(config-time-range)# absolute start 8:00 1 january 2006
\]
The following is an example of a weekly periodic time range from 8:00 a.m. to 6:00 p.m on weekdays:
\[
ciscoasa(config)# time-range workinghours
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
\]
The following example establishes an end date for the time range, and sets a weekday period from 8 a.m. to 5 p.m., plus different hours after 5 for Monday, Wednesday, Friday compared to Tuesday, Thursday.
\[
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
\]

Monitoring Objects
To monitor objects and groups, enter the following commands:

- **show access-list**
  Displays the access list entries. Entries that include objects are also expanded out into individual entries based on the object contents.

- **show running-config object [id object_id]**
  Displays all current objects. Use the id keyword to view a single object by name.

- **show running-config object object_type**
  Displays the current objects by their type, network or service.

- **show running-config object-group [id group_id]**
  Displays all current object groups. Use the id keyword to view a single object group by name.

- **show running-config object-group grp_type**
  Displays the current object groups by their group type.
## History for Objects

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object groups</td>
<td>7.0(1)</td>
<td>Object groups simplify ACL creation and maintenance. We introduced or modified the following commands: <code>object-group protocol</code>, <code>object-group network</code>, <code>object-group service</code>, <code>object-group icmp_type</code>.</td>
</tr>
<tr>
<td>Regular expressions and policy maps</td>
<td>7.2(1)</td>
<td>Regular expressions and policy maps were introduced to be used under inspection policy maps. The following commands were introduced: <code>class-map type regex</code>, <code>regex</code>, <code>match regex</code>.</td>
</tr>
<tr>
<td>Objects</td>
<td>8.3(1)</td>
<td>Object support was introduced. We introduced or modified the following commands: <code>object-network</code>, <code>object-service</code>, <code>object-group network</code>, <code>object-group service</code>, <code>network object</code>, <code>access-list extended</code>, <code>access-list webtype</code>, <code>access-list remark</code>.</td>
</tr>
<tr>
<td>User Object Groups for Identity Firewall</td>
<td>8.4(2)</td>
<td>User object groups for identity firewall were introduced. We introduced the following commands: <code>object-network user</code>, <code>user</code>.</td>
</tr>
<tr>
<td>Security Group Object Groups for Cisco TrustSec</td>
<td>8.4(2)</td>
<td>Security group object groups for Cisco TrustSec were introduced. We introduced the following commands: <code>object-network security</code>, <code>security</code>.</td>
</tr>
<tr>
<td>Mixed IPv4 and IPv6 network object groups</td>
<td>9.0(1)</td>
<td>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.</td>
</tr>
<tr>
<td>Extended ACL and object enhancement to filter ICMP traffic by ICMP code</td>
<td>9.0(1)</td>
<td>ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following commands: <code>access-list extended</code>, <code>service-object</code>, <code>service</code>.</td>
</tr>
</tbody>
</table>
Access Control Lists

Access control lists (ACLs) are used by many different features. When applied to interfaces or globally as access rules, they permit or deny traffic that flows through the appliance. For other features, the ACL selects the traffic to which the feature will apply, performing a matching service rather than a control service.

The following sections explain the basics of ACLs and how to configure and monitor them. Access rules, ACLs applied globally or to interfaces, are explained in more detail in the firewall configuration guide.

- About ACLs, page 18-1
- Guidelines for ACLs, page 18-5
- Configure ACLs, page 18-6
- Edit ACLs in an Isolated Configuration Session, page 18-19
- Monitoring ACLs, page 18-20
- History for ACLs, page 18-21

About ACLs

Access control lists (ACLs) identify traffic flows by one or more characteristics, including source and destination IP address, IP protocol, ports, EtherType, and other parameters, depending on the type of ACL. ACLs are used in a variety of features. ACLs are made up of one or more access control entries (ACEs).

ACL Types

The ASA uses the following types of ACLs:

- Extended ACLs—Extended ACLs are the main type that you will use. These ACLs are used for access rules to permit and deny traffic through the device, and for traffic matching by many features, including service policies, AAA rules, WCCP, Botnet Traffic Filter, and VPN group and DAP policies. See Configure Extended ACLs, page 18-7.

- EtherType ACLs—EtherType ACLs apply to non-IP layer-2 traffic in transparent firewall mode. You can use these rules to permit or drop traffic based on the EtherType value in the layer-2 packet. With EtherType ACLs, you can control the flow of non-IP traffic across the device. See Configure EtherType ACLs, page 18-18.
• Webtype ACLs—Webtype ACLs are used for filtering clientless SSL VPN traffic. These ACLs can deny access based on URLs or destination addresses. See Configure Webtype ACLs, page 18-14.

• Standard ACLs—Standard ACLs identify traffic by destination address only. There are few features that use them: route maps and VPN filters. Because VPN filters also allow extended access lists, limit standard ACL use to route maps. See Configure Standard ACLs, page 18-14.

The following table lists some common uses for ACLs and the type to use.

<table>
<thead>
<tr>
<th>Table 18-1</th>
<th>ACL Types and Common Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACL Use</strong></td>
<td><strong>ACL Type</strong></td>
</tr>
<tr>
<td>Control network access for IP traffic (routed and transparent mode)</td>
<td>Extended</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify traffic for AAA rules</td>
<td>Extended</td>
</tr>
<tr>
<td>Augment network access control for IP traffic for a given user</td>
<td>Extended, downloaded from a AAA server per user</td>
</tr>
<tr>
<td>VPN access and filtering</td>
<td>Extended</td>
</tr>
<tr>
<td></td>
<td>Standard</td>
</tr>
<tr>
<td>Identify traffic in a traffic class map for Modular Policy Framework</td>
<td>Extended</td>
</tr>
<tr>
<td>For transparent firewall mode, control network access for non-IP traffic</td>
<td>EtherType</td>
</tr>
<tr>
<td>Identify route filtering and redistribution</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Extended</td>
</tr>
<tr>
<td>Filtering for clientless SSL VPN</td>
<td>Webtype</td>
</tr>
</tbody>
</table>

**ACL Names**

Each ACL has a name or numeric ID, such as outside_in, OUTSIDE_IN, or 101. Limit the names to 241 characters or fewer. Consider using all uppercase letters to make it easier to find the name when viewing a running configuration.
Develop a naming convention that will help you identify the intended purpose of the ACL. For example, ASDM uses the convention `interface-name_purpose_direction`, such as “outside_access_in”, for an ACL applied to the “outside” interface in the inbound direction.

Traditionally, ACL IDs were numbers. Standard ACLs were in the range 1-99 or 1300-1999. extended ACLs were in the range 100-199 or 2000-2699. The ASA does not enforce these ranges, but if you want to use numbers, you might want to stick to these conventions to maintain consistency with routers running IOS Software.

### Access Control Entry Order

An ACL is made up of one or more ACEs. Unless you explicitly insert an ACE at a given line, each ACE that you enter for a given ACL name is appended to the end of the ACL.

The order of ACEs is important. When the ASA decides whether to forward or drop a packet, the ASA tests the packet against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked.

Thus, if you place a more specific rule after a more general rule, the more specific rule might never be hit. For example, if you want to permit network 10.1.1.0/24, but drop traffic from host 10.1.1.15 on that subnet, the ACE that denies 10.1.1.15 must come before the one that permits 10.1.1.0/24. If the permit 10.1.1.0/24 ACE comes first, 10.1.1.15 will be allowed, and the deny ACE will never be matched.

In an extended ACL, use the `line number` parameter on the `access-list` command to insert rules at the right location. Use the `show access-list name` command to view the ACL entries and their line numbers to help determine the right number to use. For other types of ACL, you must rebuild the ACL (or better, use ASDM) to change the order of ACEs.

### Permit/Deny vs. Match/Do Not Match

Access control entries either “permit” or “deny” traffic that matches the rule. When you apply an ACL to a feature that determines whether traffic is allowed through the ASA or is dropped, such as global and interface access rules, “permit” and “deny” mean what they say.

For other features, such as service policy rules, “permit” and “deny” actually mean “match” or “do not match.” In these cases, the ACL is selecting the traffic that should receive the services of that feature, such as application inspection or redirection to a service module. “Denied” traffic is simply traffic that does not match the ACL, and thus will not receive the service.

### Access Control Implicit Deny

All ACLs have an implicit deny statement at the end. Thus, for traffic controlling ACLs such as those applied to interfaces, if you do not explicitly permit a type of traffic, that traffic is dropped. For example, if you want to allow all users to access a network through the ASA except for one or more particular addresses, then you need to deny those particular addresses and then permit all others.

For ACLs used to select traffic for a service, you must explicitly “permit” the traffic; any traffic not “permitted” will not be matched for the service; “denied” traffic bypasses the service.

For EtherType ACLs, the implicit deny at the end of the ACL does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the ACL does not now block any IP traffic that you previously allowed with an extended ACL (or implicitly allowed from a high security
interface to a low security interface). However, if you explicitly deny all traffic with an EtherType ACE, then IP and ARP traffic is denied; only physical protocol traffic, such as auto-negotiation, is still allowed.

**IP Addresses Used for Extended ACLs When You Use NAT**

When you use NAT or PAT, you are translating addresses or ports, typically mapping between internal and external addresses. If you need to create an extended ACL that applies to addresses or ports that have been translated, you need to determine whether to use the real (untranslated) addresses or ports or the mapped ones. The requirement differs by feature.

Using the real address and port means that if the NAT configuration changes, you do not need to change the ACLs.

**Features That Use Real IP Addresses**

The following commands and features use real IP addresses in the ACLs, even if the address as seen on an interface is the mapped address:

- Access Rules (extended ACLs referenced by the `access-group` command)
- Service Policy Rules (Modular Policy Framework `match access-list` command)
- Botnet Traffic Filter traffic classification (`dynamic-filter enable classify-list` command)
- AAA Rules (`aaa ... match` commands)
- WCCP (`wccp redirect-list group-list` command)

For example, if you configure NAT for an inside server, 10.1.1.5, so that it has a publicly routable IP address on the outside, 209.165.201.5, then the access rule to allow the outside traffic to access the inside server needs to reference the server’s real IP address (10.1.1.5), and not the mapped address (209.165.201.5).

```plaintext
ciscoasa(config)# object network server1
ciscoasa(config-network-object)# host 10.1.1.5
ciscoasa(config-network-object)# nat (inside, outside) static 209.165.201.5

ciscoasa(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www

ciscoasa(config)# access-group OUTSIDE in interface outside
```

**Features That Use Mapped IP Addresses**

The following features use ACLs, but these ACLs use the mapped values as seen on an interface:

- IPsec ACLs
- `capture` command ACLs
- Per-user ACLs
- Routing protocol ACLs
- All other feature ACLs.

**Time-Based ACEs**

You can apply time range objects to extended and webtype ACEs so that the rules are active for specific time periods only. These types of rules let you differentiate between activity that is acceptable at certain times of the day but that is unacceptable at other times. For example, you could provide additional
restrictions during working hours, and relax them after work hours or at lunch. Conversely, you could essentially shut your network down during non-work hours. For information on creating time range objects, see Configure Time Ranges, page 17-9.

Note

Users could experience a delay of approximately 80 to 100 seconds after the specified end time for the ACL to become inactive. For example, if the specified end time is 3:50, because the end time is inclusive, the command is picked up anywhere between 3:51:00 and 3:51:59. After the command is picked up, the ASA finishes any currently running task and then services the command to deactivate the ACL.

Guidelines for ACLs

Firewall Mode Guidelines
Extended and standard ACLs are supported in routed and transparent firewall modes.
Webtype ACLs are supported in routed mode only.
EtherType ACLs are supported in transparent mode only.

Failover and Clustering Guidelines
Configuration sessions are not synchronized across failover or clustered units. When you commit the changes in a session, they are made in all failover and cluster units as normal.

IPv6 Guidelines
Extended and webtype ACLs allow a mix of IPv4 and IPv6 addresses.
Standard ACLs do not allow IPv6 addresses.
EtherType ACLs do not contain IP addresses.

(Extended ACL only.) Features That Do Not Support Identity Firewall, FQDN, and Cisco TrustSec ACLs
The following features use ACLs, but cannot accept an ACL with identity firewall (specifying user or group names), FQDN (fully-qualified domain names), or Cisco TrustSec values:

- route-map command
- VPN crypto map command
- VPN group-policy command, except for vpn-filter
- WCCP
- DAP

Additional Guidelines and Limitations
- When you specify a network mask, the method is different from the Cisco IOS software access-list command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
- Normally, you cannot reference an object or object group that does not exist in an ACL or object group, or delete one that is currently referenced. You also cannot reference an ACL that does not exist in an access-group command (to apply access rules). However, you can change this default behavior so that you can “forward reference” objects or ACLs before you create them. Until you create the objects or ACLs, any rules or access groups that reference them are ignored. To enable forward referencing, use the forward-reference enable command.
Configure ACLs

The following sections explain how to configure the various types of ACL. Read the section on ACL basics to get the big picture, then the sections on specific types of ACL for the details.

- Basic ACL Configuration and Management Options, page 18-6
- Configure Extended ACLs, page 18-7
- Configure Standard ACLs, page 18-14
- Configure Webtype ACLs, page 18-14
- Configure EtherType ACLs, page 18-18

Basic ACL Configuration and Management Options

An ACL is made up of one or more access control entries (ACEs) with the same ACL ID or name. To create a new ACL, you simply create an ACE with a new ACL name, and it becomes the first rule in the new ACL.

Working with an ACL, you can do the following things:

- Examine the ACL contents and determine line numbers and hit counts—Use the show access-list name command to view the contents of the ACL. Each row is an ACE, and includes the line number, which you will need to know if you want to insert new entries into an extended ACL. The information also includes a hit count for each ACE, which is how many times the rule was matched by traffic. For example:

  ciscoasa# show access-list outside_access_in
  access-list outside_access_in; 3 elements; name hash: 0x6892a938
  access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
  (hitcnt=0) 0xcc48b55c
  access-list outside_access_in line 2 extended permit ip host 2001:DB8::0DB8:800:200C:417A any
  (hitcnt=0) 0x79797f94
  access-list outside_access_in line 3 extended permit ip user-group LOCAL\usergroup
  any any (hitcnt=0) 0xb0f5b1e1

- Add an ACE—The command for adding an ACE is access-list name [line line-num] type parameters. The line number argument works for extended ACLs only. If you include the line number, the ACE is inserted at that location in the ACL, and the ACE that was at that location is moved down, along with the remainder of the ACEs (that is, inserting an ACE at a line number does not replace the old ACE at that line). If you do not include a line number, the ACE is added to the end of the ACL. The parameters available differ based on the ACL type; see the specific topics on each ACL type for details.

- Add comments to an ACL (all types except webtype)—Use the access-list name [line line-num] remark text command to add remarks into an ACL to help explain the purpose of an ACE. Best practice is to insert the remark before the ACE; if you view the configuration in ASDM, remarks will be associated with the ACE that follows the remarks. You can enter multiple remarks before an ACE to include an expanded comment. Each remark is limited to 100 characters. You can include leading spaces to help set off the remarks. If you do not include a line number, the remark is added to the end of the ACL. For example, you could add remarks before adding each ACE:

  ciscoasa(config)# access-list OUT remark - this is the inside admin address
  ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.3 any
  ciscoasa(config)# access-list OUT remark - this is the hr admin address
  ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.4 any
Configure ACLs

• **Edit or move an ACE or remark**—You cannot edit or move an ACE or remark. Instead, you must create a new ACE or remark with the desired values at the right location (using the line number), then delete the old ACE or remark. Because you can insert ACEs in extended ACLs only, you need to rebuild standard, webtype, or EtherType ACLs if you need to edit or move ACEs. It is far easier to reorganize a long ACL using ASDM.

• **Delete an ACE or remark**—Use the `no access-list` command to remove an ACE or remark. Use the `show access-list` command to view the parameter string that you must enter: the string must exactly match an ACE or remark to delete it, with the exception of the `line line-num` argument, which is optional on the `no access-list` command.

• **Delete an entire ACL, including remarks**—Use the `clear configure access-list name` command. USE CAUTION! The command does not ask you for confirmation. If you do not include a name, every access list on the ASA is removed.

• **Rename an ACL**—Use the `access-list name rename new_name` command.

• **Apply the ACL to a policy**—Creating an ACL in and of itself does nothing to traffic. You must apply the ACL to a policy. For example, you can use the `access-group` command to apply an extended ACL to an interface, thus denying or permitting traffic that goes through the interface. For information on some of the uses of ACLs, see ACL Types, page 18-1.

Configure Extended ACLs

An extended ACL is composed of all ACEs with the same ACL ID or name. Extended ACLs are the most complex and feature-rich type of ACL, and you can use them for many features. The most noteworthy use of extended ACLs is as access groups applied globally or to interfaces, which determine the traffic that will be denied or permitted to flow through the box. But extended ACLs are also used to determine the traffic to which other services will be provided.

Because extended ACLs are complex, the following sections focus on creating ACEs to provide specific types of traffic matching. The first sections, on basic address-based ACEs and on TCP/UDP ACEs, build the foundation for the remaining sections.

• **Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching, page 18-7**
• **Add an Extended ACE for TCP or UDP-Based Matching, with Ports, page 18-9**
• **Add an Extended ACE for ICMP-Based Matching, page 18-10**
• **Add an Extended ACE for User-Based Matching (Identity Firewall), page 18-11**
• **Add an Extended ACE for Security Group-Based Matching (Cisco TrustSec), page 18-12**
• **Examples for Extended ACLs, page 18-12**
• **Example of Converting Addresses to Objects for Extended ACLs, page 18-13**

Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching

The basic extended ACE matches traffic based on source and destination addresses, including IPv4 and IPv6 addresses and fully-qualified domain names (FQDN), such as www.example.com. In fact, every type of extended ACE must include some specification for source and destination address, so this topic explains the minimum extended ACE.

**Tip**
If you want to match traffic based on FQDN, you must create a network object for each FQDN.
To add an ACE for IP address or FQDN matching, use the following command:

```
access-list access_list_name [line line_number] extended {deny | permit}
protocol_argument source_address_argument dest_address_argument
[log {[[level] [interval secs] | disable | default]}]
[time-range time_range_name]
[inactive]
```

Example:

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

The options are:

- `access_list_name`—The name of the new or existing ACL.
- Line number—The `line line_number` option specifies the line number at which insert the ACE; otherwise, the ACE is added to the end of the ACL.
- Permit or Deny—The `deny` keyword denies or exempts a packet if the conditions are matched. The `permit` keyword permits or includes a packet if the conditions are matched.
- Protocol—The `protocol_argument` specifies the IP protocol:
  - `name` or `number`—Specifies the protocol name or number. Specify `ip` to apply to all protocols. For a list of supported keywords, see Protocols and Applications, page 43-10.
  - `object-group protocol_grp_id`—Specifies a protocol object group created using the `object-group protocol` command. See Configure Service Objects and Service Groups, page 17-4.
  - `object service_obj_id`—Specifies a service object created using the `object service` command. A TCP, UDP, or ICMP service object can include a protocol and a source or destination port or ICMP type and code.
  - `object-group service_grp_id`—Specifies a service object group created using the `object-group service` command.
- Source Address, Destination Address—The `source_address_argument` specifies the IP address or FQDN from which the packet is being sent, and the `dest_address_argument` specifies the IP address or FQDN to which the packet is being sent:
  - `host ip_address`— Specifies an IPv4 host address.
  - `ip_address mask`— Specifies an IPv4 network address and subnet mask, such as 10.100.10.0 255.255.255.0.
  - `ipv6-address/prefix-length`— Specifies an IPv6 host or network address and prefix.
  - `any`, `any4`, and `any6`— `any` specifies both IPv4 and IPv6 traffic; `any4` specifies IPv4 traffic only; and `any6` specifies IPv6 traffic only.
  - `interface interface_name`— Specifies the name of an ASA interface. Use the interface name rather than IP address to match traffic based on which interface is the source or destination of the traffic.
  - `object-group nw_grp_id`— Specifies a network object group created using the `object-group network` command.
Logging—log arguments set logging options when an ACE matches a packet for network access (an ACL applied with the access-group command). If you enter the log option without any arguments, you enable syslog message 106100 at the default level (6) and for the default interval (300 seconds). Log options are:

- level—A severity level between 0 and 7. The default is 6 (informational). If you change this level for an active ACE, the new level applies to new connections; existing connections continue to be logged at the previous level.
- interval secs—The time interval in seconds between syslog messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow from the cache used to collect drop statistics.
- disable—Disables all ACE logging.
- default—Enables logging to message 106023 for denied packets. This setting is the same as not including the log option.

Time Range—The time-range time_range_name option specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active.

Activation—Use the inactive option to disable the ACE without deleting it. To reenable it, enter the entire ACE without the inactive keyword.

Add an Extended ACE for TCP or UDP-Based Matching, with Ports

The TCP/UDP extended ACE is just the basic address-matching ACE where the protocol is tcp or udp. Because these protocols use ports, you can add port specifications to the ACE. For example, you can target HTTP traffic on TCP port 80.

To add an ACE for IP address or FQDN matching, where the protocol is TCP or UDP, use the following command:

```
access-list access_list_name [line line_number] extended (deny | permit) (tcp | udp) source_address_argument [port_argument] dest_address_argument [port_argument] [log [[level] [interval secs] | disable | default]] [time-range time_range_name] [inactive]
```

Example:

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

The port_argument option specifies the source or destination port. If you do not specify ports, all ports are matched. Available arguments include:

- operator port—The operator can be one of the following:
  - lt—less than
  - gt—greater than
  - eq—equal to
  - neq—not equal to
  - range—an inclusive range of values. When you use this operator, specify two port numbers, for example:
    
    range 100 200
The `port` can be the integer or name of a TCP or UDP port. DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP.

- **object service_obj_id**—Specifies a service object created using the `object service` command. See Configure Service Objects and Service Groups, page 17-4.

- **object-group service_grp_id**—Specifies a service object group created using the `object-group service` command.

For an explanation of the other keywords, see Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching, page 18-7.

### Add an Extended ACE for ICMP-Based Matching

The ICMP extended ACE is just the basic address-matching ACE where the protocol is `icmp` or `icmp6`. Because these protocols have type and code values, you can add type and code specifications to the ACE. For example, you can target ICMP Echo Request traffic (pings).

To add an ACE for IP address or FQDN matching, where the protocol is ICMP or ICMP6, use the following command:

```
access-list access_list_name [line line_number] extended {deny | permit} {icmp | icmp6} source_address_argument dest_address_argument [icmp_argument] [log [[level] [interval secs] | disable | default]] [time-range time_range_name] [inactive]
```

**Example:**

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

The `icmp_argument` option specifies the ICMP type and code.

- **icmp_type [icmp_code]**—Specifies the ICMP type by name or number, and the optional ICMP code for that type. If you do not specify the code, then all codes are used. For a list of ICMP types, see ICMP Types, page 43-15.

- **object-group icmp_grp_id**—Specifies an object group for ICMP/ICMP6 created using the `object-group service` or (deprecated) `object-group icmp` command.

For an explanation of the other keywords, see Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching, page 18-7.
Add an Extended ACE for User-Based Matching (Identity Firewall)

The user-based extended ACE is just the basic address-matching ACE where you include username or user group to the source matching criteria. By creating rules based on user identity, you can avoid tying rules to static host or network addresses. For example, if you define a rule for user1, and the identity firewall feature maps that user to a host assigned 10.100.10.3 one day, but 192.168.1.5 the next day, the user-based rule still applies.

Because you must still supply source and destination addresses, broaden the source address to include the likely addresses that will be assigned to the user (normally through DHCP). For example, user “LOCAL\user1 any” will match the LOCAL\user1 user no matter what address is assigned, whereas “LOCAL\user1 10.100.1.0 255.255.255.0” matches the user only if the address is on the 10.100.1.0/24 network.

By using group names, you can define rules based on entire classes of users, such as students, teachers, managers, engineers, and so forth.

To add an ACE for user or group matching, use the following command:

```
access-list access_list_name [line line_number] extended (deny | permit) protocol_argument
[user_argument] source_address_argument [port_argument]
dest_address_argument [port_argument]
[log [([level] [interval secs] | disable | default])
[time-range time_range_name]
[inactive]
```

Example:
```
ciscoasa(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

The `user_argument` option specifies the user or group for which to match traffic in addition to the source address. Available arguments include the following:

- `object-group-user user_obj_grp_id`—Specifies a user object group created using the `object-group user` command.
- `user {[(domain.nickname)\name | any | none]`— Specifies a username. Specify `any` to match all users with user credentials, or `none` to match addresses that are not mapped to usernames. These options are especially useful for combining `access-group` and `aaa authentication match` policies.
- `user-group [(domain.nickname)\user_group_name`—Specifies a user group name. Note the double \ separating the domain and group name.

For an explanation of the other keywords, see Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching, page 18-7.

**Tip**
You can include both user and Cisco Trustsec security groups in a given ACE. See Add an Extended ACE for Security Group-Based Matching (Cisco TrustSec), page 18-12.
Add an Extended ACE for Security Group-Based Matching (Cisco TrustSec)

The security group (Cisco TrustSec) extended ACE is just the basic address-matching ACE where you include security groups or tags to the source or destination matching criteria. By creating rules based on security groups, you can avoid tying rules to static host or network addresses. Because you must still supply source and destination addresses, broaden the addresses to include the likely addresses that will be assigned to users (normally through DHCP).

Before adding this type of ACE, configure Cisco TrustSec as described in Chapter 33, “ASA and Cisco TrustSec.”

To add an ACE for security group matching, use the following command:

```bash
access-list access_list_name [line line_number] extended (deny | permit) protocol_argument
[security_group_argument] source_address_argument [port_argument]
[security_group_argument] dest_address_argument [port_argument] [log [[level]
[interval secs] | disable | default]] [inactive | time-range time_range_name]
```

Example:

```bash
ciscoasa(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

The `security_group_argument` option specifies the security group for which to match traffic in addition to the source or destination address. Available arguments include the following:

- `object-group-security security_obj grp_id`—Specifies a security object group created using the `object-group security` command.
- `security-group {name security_grp_id | tag security_grp_tag}`—Specifies a security group name or tag.

For an explanation of the other keywords, see Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching, page 18-7.

You can include both user and Cisco TrustSec security groups in a given ACE. See Add an Extended ACE for User-Based Matching (Identity Firewall), page 18-11.

Examples for Extended ACLs

The following ACL allows all hosts (on the interface to which you apply the ACL) to go through the ASA:

```bash
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following ACL prevents hosts on 192.168.1.0/24 from accessing the 209.165.201.0/27 network for TCP-based traffic. All other addresses are permitted.

```bash
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

If you want to restrict access to selected hosts only, then enter a limited permit ACE. By default, all other traffic is denied unless explicitly permitted.

```bash
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```
The following ACL restricts all hosts (on the interface to which you apply the ACL) from accessing a website at address 209.165.201.29. All other traffic is allowed.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following ACL that uses object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

The following example temporarily disables an ACL that permits traffic from one group of network objects (A) to another group of network objects (B):

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

To implement a time-based ACE, use the `time-range` command to define specific times of the day and week. Then use the `access-list extended` command to bind the time range to an ACE. The following example binds an ACE in the “Sales” ACL to a time range named “New_York_Minute.”

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host 209.165.201.1 time-range New_York_Minute
```

The following example shows a mixed IPv4/IPv6 ACL:

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0 255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

### Example of Converting Addresses to Objects for Extended ACLs

The following normal ACL that does not use object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78 eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78 eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```
If you make two network object groups, one for the inside hosts, and one for the web servers, then the configuration can be simplified and can be easily modified to add more hosts:

```cisco
access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
access-list ACL_IN extended permit ip any any
access-group ACL_IN in interface inside
```

**Configure Standard ACLs**

A standard ACL is composed of all ACEs with the same ACL ID or name. Standard ACLs are used for a limited number of features, such as route maps or VPN filters. A standard ACL uses IPv4 addresses only, and defines destination addresses only.

To add a standard access list entry, use the following command:

```cisco
access-list access_list_name standard (deny | permit) {any4 | host ip_address | ip_address mask}
```

Example:

```cisco
access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

The options are:

- **Name**—The `access_list_name` argument specifies the name of number of an ACL. Traditional numbers for standard ACLs are 1-99 or 1300-1999, but you can use any name or number. You create a new ACL if the ACL does not already exist, otherwise, you are adding the entry to the end of the ACL.

- **Permit or Deny**—The `deny` keyword denies or exempts a packet if the conditions are matched. The `permit` keyword permits or includes a packet if the conditions are matched.

- **Destination Address**—The `any4` keyword matches all IPv4 addresses. The `host ip_address` argument matches a host IPv4 address. The `ip_address ip_mask` argument matches an IPv4 subnet, for example, 10.1.1.0 255.255.255.0.

**Configure Webtype ACLs**

Webtype ACLs are used for filtering clientless SSL VPN traffic, constraining user access to specific networks, subnets, hosts, and Web servers. If you do not define a filter, all connections are allowed. A webtype ACL is composed of all ACEs with the same ACL ID or name.

With webtype ACLs, you can match traffic based on URLs or destination addresses. A single ACE cannot mix these specifications. The following sections explain each type of ACE.

- Add a Webtype ACE for URL Matching, page 18-15
- Adding a Webtype ACE for IP Address Matching, page 18-16
Examples for Webtype ACLs, page 18-17

Add a Webtype ACE for URL Matching

To match traffic based on the URL the user is trying to access, use the following command;

```
access-list access_list_name webtype {deny | permit} url (url_string | any)
    [log [{level} {interval secs} | disable | default]}
    [time_range time_range_name]}
    [inactive]
```

Example:

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

The options are:

- **access_list_name**—The name of the new or existing ACL. If the ACL already exists, you are adding the ACE to the end of the ACL.
- **Permit or Deny**—The deny keyword denies or exempts a packet if the conditions are matched. The permit keyword permits or includes a packet if the conditions are matched.
- **URL**—The url keyword specifies the URL to match. Use url any to match all URL-based traffic. Otherwise, enter a URL string, which can include wildcards. Following are some tips and limitations on specifying URLs:
  - Specify any to match all URLs.
  - ‘Permit url any’ will allow all the URLs that have the format protocol://server-ip/path and will block traffic that does not match this pattern, such as port-forwarding. There should be an ACE to allow connections to the required port (port 1494 in the case of Citrix) so that an implicit deny does not occur.
  - Smart tunnel and ica plug-ins are not affected by an ACL with ‘permit url any’ because they match smart-tunnel:// and ica:// types only.
  - You can use these protocols: cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel://, and smtp://. You can also use wildcards in the protocol; for example, htt* matches http and https, and an asterisk * matches all protocols. For example, *://*.example.com matches any type URL-based traffic to the example.com network.
  - If you specify a smart-tunnel:// URL, you can include the server name only. The URL cannot contain a path. For example, smart-tunnel://www.example.com is acceptable, but smart-tunnel://www.example.com/index.html is not.
  - An asterisk * matches none or any number of characters. To match any http URL, enter http://*/
  - A question mark ? matches any one character exactly.
  - Square brackets [] are range operators, matching any character in the range. For example, to match both http://www.cisco.com:80/ and http://www.cisco.com:81/, enter http://www.cisco.com:8[01]/.
- **Logging**—log arguments set logging options when an ACE matches a packet. If you enter the log option without any arguments, you enable syslog message 106102 at the default level (6) and for the default interval (300 seconds). Log options are:
  - **level**—A severity level between 0 and 7. The default is 6.
  - **interval secs**—The time interval in seconds between syslog messages, from 1 to 600. The default is 300.
Configure ACLs

- **disable**—Disables all ACL logging.
- **default**—Enables logging to message 106103. This setting is the same as not including the `log` option.

- **Time Range**—The `time-range time_range_name` option specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active.
- **Activation**—Use the `inactive` option to disable the ACE without deleting it. To reenable it, enter the entire ACE without the inactive keyword.

## Adding a Webtype ACE for IP Address Matching

You can match traffic based on the destination address the user is trying to access. The webtype ACL can include a mix of IPv4 and IPv6 addresses in addition to URL specifications.

To add a webtype ACE for IP address matching, use the following command:

```
access-list access_list_name webtype (deny | permit) tcp dest_address_argument [operator port]
[log [[level] [interval secs] | disable | default]]
[time_range time_range_name]
[inactive]
```

**Example:**

```
ciscoasa(config)# access-list acl_company webtype permit tcp any
```

For an explanation of keywords not explained here, see Add a Webtype ACE for URL Matching, page 18-15. Keywords and arguments specific to this type of ACE include the following:

- **tcp**—The TCP protocol. Webtype ACLs match TCP traffic only.
- **Destination Address**—The `dest_address_argument` specifies the IP address to which the packet is being sent:
  - **host ip_address**—Specifies an IPv4 host address.
  - **dest_ip_address mask**—Specifies an IPv4 network address and subnet mask, such as 10.100.10.0 255.255.255.0.
  - **ipv6-address/prefix-length**—Specifies an IPv6 host or network address and prefix.
  - **any, any4, and any6**—any specifies both IPv4 and IPv6 traffic; any4 specifies IPv4 traffic only; and any6 specifies IPv6 traffic only.
- **operator port**—The destination port. If you do not specify ports, all ports are matched. The `operator` can be one of the following:
  - **lt**—less than
  - **gt**—greater than
  - **eq**—equal to
  - **neq**—not equal to
  - **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example:
    ```
    range 100 200
    ```
  The `port` can be the integer or name of a TCP port.
Examples for Webtype ACLs

The following example shows how to deny access to a specific company URL:

ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com

The following example shows how to deny access to a specific web page:

ciscoasa(config)# access-list acl_file webtype deny url https://www.example.com/dir/file.html

The following example shows how to deny HTTP access to any URL on a specific server through port 8080:

ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*

The following examples show how to use wildcards in webtype ACLs.

- The following example matches URLs such as http://www.example.com/layouts/1033:

  access-list VPN-Group webtype permit url http://www.example.com/*

- The following example matches URLs such as http://www.example.com/ and http://www.example.net/:

  access-list test webtype permit url http://www.example.*

- The following example matches URLs such as http://www.example.com and ftp://www.example.com:

  access-list test webtype permit url *://www.e*co*/

- The following example matches URLs such as http://www.cisco.com:80 and https://www.cisco.com:81:

  access-list test webtype permit url *://ww?.c*co*:8[01]/

  The range operator “[]” in the preceding example specifies that either character 0 or 1 can occur at that location.

- The following example matches URLs such as http://www.example.com and http://www.example.net:

  access-list test webtype permit url http://www.[a-z]ample?*

  The range operator “[]” in the preceding example specifies that any character in the range from a to z can occur.

- The following example matches http or https URLs that include “cgi” somewhere in the file name or path.

  access-list test webtype permit url htt*://*/*cgi*

  To match any http URL, you must enter http://*/* instead of http://*.

The following example shows how to enforce a webtype ACL to disable access to specific CIFS shares.

In this scenario we have a root folder named “shares” that contains two sub-folders named “Marketing_Reports” and “Sales_Reports.” We want to specifically deny access to the “shares/Marketing_Reports” folder.

access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
Configure EtherType ACLs

EtherType ACLs apply to non-IP layer-2 traffic in transparent firewall mode. You can use these rules to permit or drop traffic based on the EtherType value in the layer-2 packet. With EtherType ACLs, you can control the flow of non-IP traffic across the ASA. Note that 802.3-formatted frames are not handled by the ACL because they use a length field as opposed to a type field.

To add an EtherType ACE, use the following command:

```
access-list access_list_name ethertype {deny | permit} {ipx | bpdu | mpls-unicast | mpls-multicast | isis | any | hex_number}
```

Example:
```
ciscoasa(config)# access-list ETHER ethertype deny ipx
```

The options are:
- `access_list_name`—The name of the new or existing ACL. If the ACL already exists, you are adding the ACE to the end of the ACL.
- Permit or Deny—The `deny` keyword denies a packet if the conditions are matched. The `permit` keyword permits a packet if the conditions are matched.
- Traffic Matching Criteria—You can match traffic using the following options:
  - `ipx`—Internet Packet Exchange (IPX).
  - `bpdu`—bridge protocol data units, which are allowed by default.
  - `mpls-multicast`— MPLS multicast.
  - `mpls-unicast`—MPLS unicast.
  - `any`—Matches all traffic.
  - `hex_number`—Any EtherType that can be identified by a 16-bit hexadecimal number 0x600 to 0xffff. See RFC 1700, “Assigned Numbers,” at http://www.ietf.org/rfc/rfc1700.txt for a list of EtherTypes.

Examples for EtherType ACLs

The following examples shows how to configure EtherType ACLs, including how to apply them to an interface.

The following sample ACL allows common traffic originating on the inside interface:
```
ciscoasa(config)# access-list ETHER ethertype permit ipx
```
```
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
```
```
ciscoasa(config)# access-group ETHER in interface inside
```
The following ACL allows some EtherTypes through the ASA, but it denies IPX:

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
```
```
ciscoasa(config)# access-list ETHER ethertype permit 1234
```
```
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
```
```
ciscoasa(config)# access-group ETHER in interface inside
```
```
ciscoasa(config)# access-group ETHER in interface outside
```

The following ACL denies traffic with EtherType 0x1256, but it allows all others on both interfaces:

```
ciscoasa(config)# access-list nonIP ethertype deny 1256
```
```
ciscoasa(config)# access-list nonIP ethertype permit any
```
```
ciscoasa(config)# access-group ETHER in interface inside
```
```
ciscoasa(config)# access-group ETHER in interface outside
```

## Edit ACLs in an Isolated Configuration Session

When you edit an ACL used for access rules or any other purpose, the change is immediately implemented and impacts traffic. With access rules, you can enable the transactional commit model to ensure that new rules become active only after rule compilation is complete, but the compilation happens after each ACE you edit.

If you want to further isolate the impact of editing ACLs, you can make your changes in a “configuration session,” which is an isolated mode that allows you to edit several ACEs and objects before explicitly committing your changes. Thus, you can ensure that all of your intended changes are complete before you change device behavior.

### Before You Begin
- You can edit ACLs that are referenced by an access-group command, but you cannot edit ACLs that are referenced by any other command. You can also edit unreferenced ACLs or create new ones.
- You can create or edit objects and object groups, but if you create one in a session, you cannot edit it in the same session. If the object is not defined as desired, you must commit your changes and then edit the object, or discard the entire session and start over.
- When you edit an ACL that is referenced by an access-group command (access rules), the transactional commit model is used when you commit the session. Thus, the ACL is completely compiled before the new version replaces the old version.
- If you enable forward referencing of ACL and object names (the `forward-reference enable` command), you can delete an ACL that is referenced by an access-group command (access rules), and then recreate the ACL. When you commit changes, the new version of the ACL will be used after compilation is complete. You can also create rules that refer to objects that do not exist, or delete objects that are in use by access rules. However, you will get a commit error if you delete an object used by other rules, such as NAT.

### Procedure

#### Step 1
Start the session.
```
ciscoasa# configure session session_name
```
```
ciscoasa(config-s)#
```

If the `session_name` already exists, you open that session. Otherwise, you are creating a new session.
Use the `show configuration session` command to view the existing sessions. You can have at most 3 sessions active at a time. If you need to delete an old unused session, use the `clear configuration session session_name` command.

If you cannot open an existing session because someone else is editing it, you can clear the flag that indicates the session is being edited. Do this only if you are certain the session is not actually being edited. Use the `clear session session_name access` command to reset the flag.

**Step 2**
(Uncommitted sessions only.) Make your changes. You can use the following basic commands with any of their parameters:

- `access-list`
- `object`
- `object-group`

**Step 3**
Decide what to do with the session. The commands available depend on whether you have previously committed the session. Possible commands are:

- `exit`—To simply exit the session without committing or discarding changes, so that you can return later.

- `commit [noconfirm | revert-save | config-save]`—(Uncommitted sessions only.) To commit your changes. You are asked if you want to save the session. You can save the revert session (`revert-save`), which lets you undo your changes using the `revert` command, or the configuration session (`config-save`), which includes all of the changes made in the session (allowing you to commit the same changes again if you would like to). If you save the revert or configuration session, the changes are committed, but the session remains active. You can open the session and revert or recommit the changes. You can avoid the prompt by including the `noconfirm` option and optionally, the desired save option.

- `abort`—(Uncommitted sessions only.) To abandon your changes and delete the session. If you want to keep the session, exit the session and use the `clear session session_name configuration` command, which empties the session without deleting it.

- `revert`—(Committed sessions only.) To undo your changes, returning the configuration back to what it was before you committed the session, and delete the session.

- `show configuration session [session_name]`—To show the changes made in the session.

### Monitoring ACLs

To monitor ACLs, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show access-list [name]</code></td>
<td>Displays the access lists, including the line number for each ACE and hit counts. Include an ACL name or you will see all access lists.</td>
</tr>
<tr>
<td><code>show running-config access-list [name]</code></td>
<td>Displays the current running access-list configuration. Include an ACL name or you will see all access lists.</td>
</tr>
</tbody>
</table>
# History for ACLs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended, standard, webtype ACLs</td>
<td>7.0(1)</td>
<td>ACLs are used to control network access or to specify traffic for many features to act upon. An extended access control list is used for through-the-box access control and several other features. Standard ACLs are used in route maps and VPN filters. Webtype ACLs are used in clientless SSL VPN filtering. EtherType ACLs control non-IP layer 2 traffic. We introduced the following commands: <code>access-list extended</code>, <code>access-list standard</code>, <code>access-list webtype</code>, <code>access-list ethtype</code>.</td>
</tr>
<tr>
<td>Real IP addresses in extended ACLs</td>
<td>8.3(1)</td>
<td>When using NAT or PAT, mapped addresses and ports are no longer used in an ACL for several features. You must use the real, untranslated addresses and ports for these features. Using the real address and port means that if the NAT configuration changes, you do not need to change the ACLs. For more information, see IP Addresses Used for Extended ACLs When You Use NAT, page 18-4.</td>
</tr>
<tr>
<td>Support for Identity Firewall in extended ACLs</td>
<td>8.4(2)</td>
<td>You can now use identity firewall users and groups for the source and destination. You can use an identity firewall ACL with access rules, AAA rules, and for VPN authentication. We modified the following commands: <code>access-list extended</code>.</td>
</tr>
<tr>
<td>EtherType ACL support for IS-IS traffic</td>
<td>8.4(5), 9.1(2)</td>
<td>In transparent firewall mode, the ASA can now control IS-IS traffic using an EtherType ACL. We modified the following command: `access-list ethertype {permit</td>
</tr>
<tr>
<td>Support for Cisco TrustSec in extended ACLs</td>
<td>9.0(1)</td>
<td>You can now use Cisco TrustSec security groups for the source and destination. You can use an identity firewall ACL with access rules. We modified the following commands: <code>access-list extended</code>.</td>
</tr>
</tbody>
</table>
### History for ACLs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified extended and webtype ACLs for IPv4 and IPv6</td>
<td>9.0(1)</td>
<td>Extended and webtype ACLs now support IPv4 and IPv6 addresses. You can even specify a mix of IPv4 and IPv6 addresses for the source and destination. The <code>any</code> keyword was changed to represent IPv4 and IPv6 traffic. The <code>any4</code> and <code>any6</code> keywords were added to represent IPv4-only and IPv6-only traffic, respectively. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs. See the release notes for more information about migration. We modified the following commands: <code>access-list extended, access-list webtype</code>. We removed the following commands: <code>ipv6 access-list, ipv6 access-list webtype, ipv6-VPN-filter</code>.</td>
</tr>
<tr>
<td>Extended ACL and object enhancement to filter ICMP traffic by ICMP code</td>
<td>9.0(1)</td>
<td>ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following commands: <code>access-list extended, service-object, service</code>.</td>
</tr>
<tr>
<td>Configuration session for editing ACLs and objects. Forward referencing of objects and ACLs in access rules.</td>
<td>9.3(2)</td>
<td>You can now edit ACLs and objects in an isolated configuration session. You can also forward reference objects and ACLs, that is, configure rules and access groups for objects or ACLs that do not yet exist. We introduced the <code>clear configuration session, clear session, configure session, forward-reference, and show configuration session</code> commands.</td>
</tr>
</tbody>
</table>
PART 6

IP Routing
Routing Overview

This chapter describes underlying concepts of how routing behaves within the Cisco ASA, and the routing protocols that are supported. Routing is the act of moving information across a network from a source to a destination. Along the way, at least one intermediate node is typically encountered. Routing involves two basic activities: determining optimal routing paths and transporting packets through a network.

- Path Determination, page 19-1
- Supported Route Types, page 19-2
- How Routing Behaves Within the ASA, page 19-3
- Supported Internet Protocols for Routing, page 19-5
- Routing Table, page 19-6
- Disable Proxy ARP Requests, page 19-10
- Display the Routing Table, page 19-11

Path Determination

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth, that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which include route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Destination or next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the next hop on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables also can include other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message sent
between routers, informs other routers of the state of the sender links. Link information also can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

**Note**  
Asymmetric routing is only supported for Active/Active failover in multiple context mode.

## Supported Route Types

There are several route types that a router can use. The ASA uses the following route types:

- Static Versus Dynamic, page 19-2
- Single-Path Versus Multipath, page 19-3
- Flat Versus Hierarchical, page 19-3
- Link-State Versus Distance Vector, page 19-3

### Static Versus Dynamic

Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Because static routing systems cannot react to network changes, they generally are considered unsuitable for large, constantly changing networks. Most of the dominant routing algorithms are dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly.

Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a router to which all unroutable packets are sent), for example, can be designated to act as a repository for all unroutable packets, ensuring that all messages are at least handled in some way.
Single-Path Versus Multipath

Some sophisticated routing protocols support multiple paths to the same destination. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines. The advantages of multipath algorithms are substantially better throughput and reliability, which is generally called load sharing.

Flat Versus Hierarchical

Some routing algorithms operate in a flat space, while others use routing hierarchies. In a flat routing system, the routers are peers of all others. In a hierarchical routing system, some routers form what amounts to a routing backbone. Packets from nonbackbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone router through one or more nonbackbone routers to the final destination.

Routing systems often designate logical groups of nodes, called domains, autonomous systems, or areas. In hierarchical systems, some routers in a domain can communicate with routers in other domains, while others can communicate only with routers within their domain. In very large networks, additional hierarchical levels may exist, with routers at the highest hierarchical level forming the routing backbone.

The primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns well. Most network communication occurs within small company groups (domains). Because intradomain routers need to know only about other routers within their domain, their routing algorithms can be simplified, and, depending on the routing algorithm being used, routing update traffic can be reduced accordingly.

Link-State Versus Distance Vector

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. Each router, however, sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables. Distance vector algorithms (also known as Bellman-Ford algorithms) call for each router to send all or some portion of its routing table, but only to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. Distance vector algorithms know only about their neighbors. Typically, link-state algorithms are used in conjunction with OSPF routing protocols.

How Routing Behaves Within the ASA

The ASA uses both routing table and XLATE tables for routing decisions. To handle destination IP translated traffic, that is, untranslated traffic, the ASA searches for existing XLATE, or static translation to select the egress interface.

- Egress Interface Selection Process, page 19-4
- Next Hop Selection Process, page 19-4
- ECMP Routing, page 19-4
Egress Interface Selection Process

The selection process follows these steps:

1. If a destination IP translating XLATE already exists, the egress interface for the packet is determined from the XLATE table, but not from the routing table.

2. If a destination IP translating XLATE does not exist, but a matching static translation exists, then the egress interface is determined from the static NAT rule and an XLATE is created, and the routing table is not used.

3. If a destination IP translating XLATE does not exist and no matching static translation exists, the packet is not destination IP translated. The ASA processes this packet by looking up the route to select the egress interface, then source IP translation is performed (if necessary).

For regular dynamic outbound NAT, initial outgoing packets are routed using the route table and then creating the XLATE. Incoming return packets are forwarded using existing XLATE only. For static NAT, destination translated incoming packets are always forwarded using existing XLATE or static translation rules.

Next Hop Selection Process

After selecting the egress interface using any method described previously, an additional route lookup is performed to find out suitable next hop(s) that belong to a previously selected egress interface. If there are no routes in the routing table that explicitly belong to a selected interface, the packet is dropped with a level 6 syslog message 110001 generated (no route to host), even if there is another route for a given destination network that belongs to a different egress interface. If the route that belongs to a selected egress interface is found, the packet is forwarded to the corresponding next hop.

Load sharing on the ASA is possible only for multiple next hops available using a single egress interface. Load sharing cannot share multiple egress interfaces.

If dynamic routing is in use on the ASA and the route table changes after XLATE creation (for example, route flap), then destination translated traffic is still forwarded using the old XLATE, not via the route table, until XLATE times out. It may be either forwarded to the wrong interface or dropped with a level 6 syslog message 110001 generated (no route to host), if the old route was removed from the old interface and attached to another one by the routing process.

The same problem may happen when there are no route flaps on the ASA itself, but some routing process is flapping around it, sending source-translated packets that belong to the same flow through the ASA using different interfaces. Destination-translated return packets may be forwarded back using the wrong egress interface.

This issue has a high probability in some security traffic configurations, where virtually any traffic may be either source-translated or destination-translated, depending on the direction of the initial packet in the flow. When this issue occurs after a route flap, it can be resolved manually by using the `clear xlate` command, or automatically resolved by an XLATE timeout. The XLATE timeout may be decreased if necessary. To ensure that this issue rarely occurs, make sure that there are no route flaps on the ASA and around it. That is, ensure that destination-translated packets that belong to the same flow are always forwarded the same way through the ASA.

ECMP Routing

The ASA supports Equal-Cost Multi-Path (ECMP) routing.
Without zones, you can have up to 3 equal cost static or dynamic routes per interface. For example, you can configure three default routes on the outside interface that specify different gateways:

route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4

In this case, traffic is load-balanced on the outside interface between 10.1.1.2, 10.1.1.3, and 10.1.1.4. Traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses.

ECMP is not supported across multiple interfaces, so you cannot define a route to the same destination on a different interface. The following route is disallowed when configured with any of the routes above:

route outside2 0 0 10.2.1.1

With zones, you can have up to 8 equal cost static or dynamic routes across up to 8 interfaces within a zone. For example, you can configure three default routes across three interfaces in the zone:

route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2

Similarly, your dynamic routing protocol can automatically configure equal cost routes. The ASA load-balances traffic across the interfaces with a more robust load balancing mechanism.

When a route is lost, the ASA seamlessly moves the flow to a different route.

**Supported Internet Protocols for Routing**

The ASA supports several Internet protocols for routing. Each protocol is briefly described in this section.

- **Enhanced Interior Gateway Routing Protocol (EIGRP)**
  
  EIGRP is a Cisco proprietary protocol that provides compatibility and seamless interoperation with IGRP routers. An automatic-redistribution mechanism allows IGRP routes to be imported into Enhanced IGRP, and vice versa, so it is possible to add Enhanced IGRP gradually into an existing IGRP network.

  For more information about configuring EIGRP, see Configure EIGRP, page 24-3.

- **Open Shortest Path First (OSPF)**
  
  OSPF is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force (IETF). OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area includes an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

  For more information about configuring OSPF, see Configure OSPFv2, page 23-6.

- **Routing Information Protocol (RIP)**

  RIP is a distance-vector protocol that uses hop count as its metric. RIP is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system.

  For more information about configuring RIP, see the legacy feature guide.

- **Border Gateway Protocol (BGP)**
BGP is an interautonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP). Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

For more information about configuring BGP, see Configure BGP, page 22-4

Routing Table

- How the Routing Table Is Populated, page 19-6
- How Forwarding Decisions Are Made, page 19-8
- Dynamic Routing and Failover, page 19-8
- Dynamic Routing and Clustering, page 19-9
- Dynamic Routing in Multiple Context Mode, page 19-9

How the Routing Table Is Populated

The ASA routing table can be populated by statically defined routes, directly connected routes, and routes discovered by the RIP, EIGRP, OSPF and BGP routing protocols. Because the ASA can run multiple routing protocols in addition to having static and connected routes in the routing table, it is possible that the same route is discovered or entered in more than one manner. When two routes to the same destination are put into the routing table, the one that remains in the routing table is determined as follows:

- If the two routes have different network prefix lengths (network masks), then both routes are considered unique and are entered into the routing table. The packet forwarding logic then determines which of the two to use.

  For example, if the RIP and OSPF processes discovered the following routes:

  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19

  Even though OSPF routes have the better administrative distance, both routes are installed in the routing table because each of these routes has a different prefix length (subnet mask). They are considered different destinations and the packet forwarding logic determines which route to use.

- If the ASA learns about multiple paths to the same destination from a single routing protocol, such as RIP, the route with the better metric (as determined by the routing protocol) is entered into the routing table.

  Metrics are values associated with specific routes, ranking them from most preferred to least preferred. The parameters used to determine the metrics differ for different routing protocols. The path with the lowest metric is selected as the optimal path and installed in the routing table. If there are multiple paths to the same destination with equal metrics, load balancing is done on these equal cost paths.

- If the ASA learns about a destination from more than one routing protocol, the administrative distances of the routes are compared, and the routes with lower administrative distance are entered into the routing table.
Administrative Distances for Routes

You can change the administrative distances for routes discovered by or redistributed into a routing protocol. If two routes from two different routing protocols have the same administrative distance, then the route with the lower default administrative distance is entered into the routing table. In the case of EIGRP and OSPF routes, if the EIGRP route and the OSPF route have the same administrative distance, then the EIGRP route is chosen by default.

Administrative distance is a route parameter that the ASA uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Because the routing protocols have metrics based on algorithms that are different from the other protocols, it is not always possible to determine the best path for two routes to the same destination that were generated by different routing protocols.

Each routing protocol is prioritized using an administrative distance value. Table 19-1 shows the default administrative distance values for the routing protocols supported by the ASA.

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Administrative Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP Summary Route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>EIGRP external route</td>
<td>170</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>255</td>
</tr>
</tbody>
</table>

The smaller the administrative distance value, the more preference is given to the protocol. For example, if the ASA receives a route to a certain network from both an OSPF routing process (default administrative distance - 110) and a RIP routing process (default administrative distance - 120), the ASA chooses the OSPF route because OSPF has a higher preference. In this case, the router adds the OSPF version of the route to the routing table.

In this example, if the source of the OSPF-derived route was lost (for example, due to a power shutdown), the ASA would then use the RIP-derived route until the OSPF-derived route reappears.

The administrative distance is a local setting. For example, if you use the `distance-ospf` command to change the administrative distance of routes obtained through OSPF, that change would only affect the routing table for the ASA on which the command was entered. The administrative distance is not advertised in routing updates.

Administrative distance does not affect the routing process. The EIGRP, OSPF, RIP and BGP routing processes only advertise the routes that have been discovered by the routing process or redistributed into the routing process. For example, the RIP routing process advertises RIP routes, even if routes discovered by the OSPF routing process are used in the ASA routing table.
Backup Routes

A backup route is registered when the initial attempt to install the route in the routing table fails because another route was installed instead. If the route that was installed in the routing table fails, the routing table maintenance process calls each routing protocol process that has registered a backup route and requests them to reinstall the route in the routing table. If there are multiple protocols with registered backup routes for the failed route, the preferred route is chosen based on administrative distance.

Because of this process, you can create floating static routes that are installed in the routing table when the route discovered by a dynamic routing protocol fails. A floating static route is simply a static route configured with a greater administrative distance than the dynamic routing protocols running on the ASA. When the corresponding route discovered by a dynamic routing process fails, the static route is installed in the routing table.

How Forwarding Decisions Are Made

Forwarding decisions are made as follows:

- If the destination does not match an entry in the routing table, the packet is forwarded through the interface specified for the default route. If a default route has not been configured, the packet is discarded.
- If the destination matches a single entry in the routing table, the packet is forwarded through the interface associated with that route.
- If the destination matches more than one entry in the routing table, and the entries all have the same network prefix length, the two entries with identical network prefixes and different interfaces cannot coexist in the routing table.
- If the destination matches more than one entry in the routing table, and the entries have different network prefix lengths, then the packet is forwarded out of the interface associated with the route that has the longer network prefix length.

For example, a packet destined for 192.168.32.1 arrives on an interface of an ASA with the following routes in the routing table:

```
ciscoasa# show route
....
R  192.168.32.0/24 [120/4] via 10.1.1.2
O  192.168.32.0/19 [110/229840] via 10.1.1.3
....
```

In this case, a packet destined to 192.168.32.1 is directed toward 10.1.1.2, because 192.168.32.1 falls within the 192.168.32.0/24 network. It also falls within the other route in the routing table, but the 192.168.32.0/24 has the longest prefix within the routing table (24 bits versus 19 bits). Longer prefixes are always preferred over shorter ones when forwarding a packet.

Dynamic Routing and Failover

Dynamic routes are synchronized on the standby unit when the routing table changes on the active unit, which means that all additions, deletions, or changes on the active unit are immediately propagated to the standby unit. If the standby unit becomes active after the primary unit has been active for a period of time, routes become synchronized as a part of the failover bulk synchronization process, so the routing table on the active/standby failover pair should appear the same.
Dynamic Routing and Clustering

Dynamic routing is fully integrated in a cluster, and routes are shared across units. Routing table entries are also replicated across units in a cluster.

When one unit transitions from the slave to the master, the epoch number (32-bit sequence number) for the RIB table is incremented. After the transition, the new master unit initially has RIB table entries that are the mirror image of the previous master unit. In addition, the reconvergence timer starts on the new master unit. When the epoch number for the RIB table is incremented, all existing entries are considered stale. Forwarding of IP packets continues as normal. On the new master unit, dynamic routing protocols start to either update existing route entries or create new route entries with the new epoch number. These modified or new entries with the current epoch number indicate that they have been refreshed and are synchronized to all slave units. After the reconvergence timer has expired, old entries from the RIB table are removed. RIB table entries for OSPF routes, RIP routes, and EIGRP routes are synchronized to the slave units.

Bulk synchronization occurs only when a unit joins a cluster and is from the master unit to a joining unit. For dynamic routing updates, when the master unit learns a new route through OSPF, RIP or EIGRP, the master unit sends those updates to all slave units through reliable message transmission. Slave units update their RIB tables after they receive a cluster route update message.

For the supported dynamic routing protocols (OSPF, RIP, and EIGRP), routing packets from Spanned EtherChannel interfaces on the slave units are forwarded to the master unit. Only the master unit sees and processes dynamic routing protocol packets. When the slave unit requests a bulk synchronization, all routing entries learned through Spanned EtherChannel interfaces are replicated.

When new routing entries are learned through Spanned EtherChannel interfaces on the master unit, the new entries are broadcast to all slave units. When existing routing entries are modified because of a network topology change, the modified entries are also synchronized to all slave units. When existing routing entries are removed because of a network topology change, the removed entries are also synchronized to all slave units.

In multiple context mode, the master-slave synchronization includes all the contexts and the RIB table entries of all the contexts in the synchronization message.

If you configure Individual interfaces, you must also configure the router-id pool setting.

Dynamic Routing in Multiple Context Mode

In multiple context mode, each context maintains a separate routing table and routing protocol databases. This enables you to configure OSPFv2 and EIGRP independently in each context. You can configure EIGRP in some contexts and OSPFv2 in the same or different contexts. In mixed context mode, you can enable any of the dynamic routing protocols in contexts that are in routed mode. RIP and OSPFv3 are not supported in multiple context mode.

The following table lists the attributes for EIGRP, OSPFv2, route maps used for distributing routes into OSPFv2 and EIGRP processes, and prefix lists used in OSPFv2 to filter the routing updates entering or leaving an area when they are used in multiple context mode:
A resource class called routes specifies the maximum number of routing table entries that can exist in a context. This resolves the problem of one context affecting the available routing table entries in another context and also allows you greater control over the maximum route entries per context.

Because there is no definitive system limit, you can only specify an absolute value for this resource limit; you may not use a percentage limit. Also, there are no minimum and maximum limits per context, so the default class does not change. If you add a new route for any of the static or dynamic routing protocols (connected, static, OSPF, EIGRP, and RIP) in a context and the resource limit for that context is exhausted, then the route addition fails and a syslog message is generated.

### Disable Proxy ARP Requests

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request asking “Who is this IP address?” The device owning the IP address replies, “I own that IP address; here is my MAC address.”

Proxy ARP is used when a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. The ASA uses proxy ARP when you configure NAT and specify a mapped address that is on the same network as the ASA interface. The only way traffic can reach the hosts is if the ASA uses proxy ARP to claim that the MAC address is assigned to destination mapped addresses.

Under rare circumstances, you might want to disable proxy ARP for NAT addresses.

If you have a VPN client address pool that overlaps with an existing network, the ASA by default sends proxy ARP requests on all interfaces. If you have another interface that is on the same Layer 2 domain, it will see the ARP requests and will answer with the MAC address of its interface. The result of this is
that the return traffic of the VPN clients towards the internal hosts will go to the wrong interface and will get dropped. In this case, you need to disable proxy ARP requests for the interface on which you do not want them.

**Procedure**

**Step 1**

Disable proxy ARP requests:

```
sysopt noproxyarp interface
```

Example:

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

**Display the Routing Table**

**Procedure**

**Step 1**

View the entries in the routing table:

```
ciscoasa# show route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

```
S  10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C  10.86.194.0 255.255.254.0 is directly connected, outside
S* 0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

Display the Routing Table
Static and Default Routes

This chapter describes how to configure static and default routes on the Cisco ASA.

- About Static and Default Routes, page 20-1
- Guidelines for Static and Default Routes, page 20-3
- Configure Default and Static Routes, page 20-3
- Monitoring a Static or Default Route, page 20-7
- Examples for Static or Default Routes, page 20-7
- History for Static and Default Routes, page 20-8

About Static and Default Routes

To route traffic to a nonconnected host or network, you must define a route to the host or network, either using static or dynamic routing. Generally, you must configure at least one static route: a default route for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

- Default Route, page 20-1
- Static Routes, page 20-2
- Route to null0 Interface to “Black Hole” Unwanted Traffic, page 20-2
- Route Priorities, page 20-2
- Transparent Firewall Mode Routes, page 20-2
- Equal-Cost Multi-Path Routes, page 20-2
- Static Route Tracking, page 20-3

Default Route

The simplest option is to configure a default route to send all traffic to an upstream router, relying on the router to route the traffic for you. A default route identifies the gateway IP address to which the ASA sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 as the destination IP address.
Static Routes

You might want to use static routes in single context mode in the following cases:

- Your networks use a different router discovery protocol from BGP, EIGRP, RIP, or OSPF.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the ASA.

Route to null0 Interface to “Black Hole” Unwanted Traffic

Access rules let you filter packets based on the information contained in their headers. A static route to the null0 interface is a complementary solution to access rules. You can use a null0 route to forward unwanted or undesirable traffic into a “black hole” so the traffic is dropped.

Static null0 routes have a favorable performance profile. You can also use static null0 routes to prevent routing loops. BGP can leverage the static null0 route for Remotely Triggered Black Hole routing.

Route Priorities

- Routes that identify a specific destination take precedence over the default route.
- When multiple routes exist to the same destination (either static or dynamic), then the administrative distance for the route determines priority. Static routes are set to 1, so they typically are the highest priority routes.
- When you have multiple static routes to the same destination with the same administrative distance, see ECMP Routing, page 19-4.
- For traffic emerging from a tunnel with the Tunneled option, this route overrides any other configured or learned default routes.

Transparent Firewall Mode Routes

In transparent firewall mode, for traffic that originates on the ASA and is destined for a nondirectly connected network, you need to configure either a default route or static routes so the ASA knows out of which interface to send traffic. Traffic that originates on the ASA might include communications to a syslog server, Websense or N2H2 server, or AAA server. If you have servers that cannot all be reached through a single default route, then you must configure static routes.

Equal-Cost Multi-Path Routes

The ASA supports Equal-Cost Multi-Path (ECMP) routing. See ECMP Routing, page 19-4 for more information.
Static Route Tracking

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the ASA goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

Guidelines for Static and Default Routes

Firewall Mode
Static route tracking is not supported in transparent firewall mode.

IPv6
- IPv6 static routes are not supported in transparent mode in ASDM.
- Static route tracking is not supported for IPv6.

Clustering
In clustering, static route monitoring is only supported on the master unit.

Configure Default and Static Routes

At a minimum, you should configure a default route. You may need to configure static routes as well.

- Configure a Default Route, page 20-3
- Configure a Static Route, page 20-4
- Track Static Routes, page 20-5

Configure a Default Route

A default route is simply a static route with 0.0.0.0/0 as the destination IP address.

Before You Begin
See the following guidelines for the Tunneled option:
- Do not enable unicast RPF (ip verify reverse-path command) on the egress interface of a tunneled route, because this setting causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route, because this setting causes the session to fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspection engine, or the DCE RPC inspection engine with tunneled routes, because these inspection engines ignore the tunneled route.
- You cannot define more than one default route with the tunneled option.
Configure Default and Static Routes

Chapter 20      Static and Default Routes

Configure Default and Static Routes

Procedure

Step 1
Add a default route:
IPv4:
route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance | tunneled]
IPv6:
ipv6 route if_name ::/0 next_hop_ipv6_addr [distance | tunneled]

Example:
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1

The if_name is the interface through which you want to send the specific traffic.
The distance argument is the administrative distance for the route, between 1 and 254. The default is 1 if you do not specify a value. Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connect routes. The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static routes take precedence. Connected routes always take precedence over static or dynamically discovered routes.

Note
If you have two default routes configured on different interfaces that have different metrics, the connection to the ASA that is made from the higher metric interface fails, but connections to the ASA from the lower metric interface succeed as expected.

You can define a separate default route for tunneled traffic along with the standard default route using the tunneled keyword. When you create a default route with the tunneled option, all traffic from a tunnel terminating on the ASA that cannot be routed using learned or static routes is sent to this route.

Tip
You can enter 0 0 instead of 0.0.0.0 0.0.0.0 for the destination network address and mask, as shown in the following example:

ciscoasa(config)# route outside 0 0 192.168.2.4

Configure a Static Route

A static route defines where to send traffic for specific destination networks.

Procedure

Step 1
Add a static route:
route  if_name  dest_ip  mask  gateway_ip  [distance]

Example:
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1

The if_name is the interface through which you want to send the specific traffic. To “black hole” unwanted traffic, enter the null0 interface.

The dest_ip and mask arguments indicate the IP address for the destination network and the gateway_ip argument is the address of the next-hop router. The addresses you specify for the static route are the addresses that are in the packet before entering the ASA and performing NAT.

The distance argument is the administrative distance for the route. The default is 1 if you do not specify a value. Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connected routes. The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static route takes precedence. Connected routes always take precedence over static or dynamically discovered routes.

Examples
The following example shows static routes for 3 networks that go to the same gateway, and another network that goes to a separate gateway:

route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1

Track Static Routes

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

- About Static Route Tracking, page 20-5
- Configure Static Route Tracking, page 20-6

About Static Route Tracking

The ASA implements static route tracking by associating a static route with a monitoring target host on the destination network that the ASA monitors using ICMP echo requests. If an echo reply is not received within a specified time period, the host is considered down, and the associated route is removed from the routing table. An untracked backup route with a higher metric is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address
- The next hop gateway address (if you are concerned about the availability of the gateway)
- A server on the target network, such as a AAA server, that the ASA needs to communicate with
Configure Default and Static Routes

Configure Static Route Tracking

To configure static route tracking, complete the following steps.

**Before You Begin**
Static route tracking is supported for:

- IPv4 traffic.
- Routed firewall mode.

**Procedure**

**Step 1** Define the monitoring process:

```
sla monitor sla_id
```

Example:

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

**Step 2** Specify the monitoring protocol, the target host on the tracked network, and the interface through which you reach the network:

```
type echo protocol ipicmpecho target_ip interface if_name
```

Example:

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134
```

The `target_ip` argument is the IP address of the network object whose availability the tracking process monitors. While this object is available, the tracking process route is installed in the routing table. When this object becomes unavailable, the tracking process removes the route and the backup route is used in its place.

**Step 3** (Optional) Configure monitoring options. See the command reference for the following commands: `frequency`, `num-packets`, `request-data-size`, `threshold`, `timeout`, and `tos`.

**Step 4** Schedule the monitoring process:

```
sla monitor schedule sla_id [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]
```

Example:

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

Typically, you will use the `sla monitor schedule sla_id life forever start-time now` command for the monitoring schedule, and allow the monitoring configuration to determine how often the testing occurs.
However, you can schedule this monitoring process to begin in the future and to only occur at specified times.

**Step 5**  
Associate a tracked static route with the SLA monitoring process:

```
track track_id rtr sla_id reachability
```

Example:

```
ciscoasa(config)# track 6 rtr 5 reachability
```

The *track_id* argument is a tracking number you assign with this command. The *sla_id* argument is the ID number of the SLA process.

**Step 6**  
Track one of the following route types:

- **Static route:**
  ```
  route if_name dest_ip mask gateway_ip [distance] track track_id
  ```

  Example:
  ```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  You cannot use the *tunneled* option.

- **Default route obtained through DHCP:**
  ```
  interface interface_id
dhcp client route track track_id
  ```

- **Default route obtained through PPPoE:**
  ```
  interface interface_id
  pppoe client route track track_id
  ```

**Step 7**  
Create an untracked backup route.

The backup route is a static route to the same destination as the tracked route, but through a different interface or gateway. You must assign this route a higher administrative distance (metric) than your tracked route.

---

### Monitoring a Static or Default Route

- **show route**
  
  Displays the routing table.

---

### Examples for Static or Default Routes

The following example shows how to create a static route that sends all traffic destined for 10.1.1.0/24 to the router 10.1.2.45, which is connected to the inside interface, defines three equal cost static routes that direct traffic to three different gateways on the dmz interface, and adds a default route for tunneled traffic and one for regular traffic.

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
```
History for Static and Default Routes

Table 20-1  Feature History for Static and Default Routes

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Route Tracking</td>
<td>7.2(1)</td>
<td>The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. We introduced the following commands: clear configure sla, frequency, num-packets, request-data-size, show sla monitor, show running-config sla, sla monitor, sla monitor schedule, threshold, timeout, tos, track rtr</td>
</tr>
<tr>
<td>Static null0 route to “black hole” traffic</td>
<td>9.2(1)</td>
<td>Sending traffic to a null0 interface results in dropping the packets destined to the specified network. This feature is useful in configuring Remotely Triggered Black Hole (RTBH) for BGP. We modified the following command: route.</td>
</tr>
</tbody>
</table>
Route Maps

- About Route Maps, page 21-1
- Guidelines for Route Maps, page 21-4
- Define a Route Map, page 21-4
- Customize a Route Map, page 21-4
- Configuration Example for Route Maps, page 21-6
- Feature History for Route Maps, page 21-7

About Route Maps

Route maps are used when redistributing routes into an OSPF, RIP, EIGRP or BGP routing process. They are also used when generating a default route into an OSPF routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Route maps have many features in common with widely known ACLs. These are some of the traits common to both:

- They are an ordered sequence of individual statements, each has a permit or deny result. Evaluation of ACL or route maps consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is aborted once the first statement match is found and an action associated with the statement match is performed.
- They are generic mechanisms—Criteria matches and match interpretation are dictated by the way that they are applied. The same route map applied to different tasks might be interpreted differently.

These are some of the differences between route maps and ACLs:

- Route maps frequently use ACLs as matching criteria.
- The main result from the evaluation of an ACL is a yes or no answer—An ACL either permits or denies input data. Applied to redistribution, an ACL determines if a particular route can (route matches ACLs permit statement) or can not (matches deny statement) be redistributed. Typical route maps not only permit (some) redistributed routes but also modify information associated with the route, when it is redistributed into another protocol.
- Route maps are more flexible than ACLs and can verify routes based on criteria which ACLs can not verify. For example, a route map can verify if the type of route is internal.
Each ACL ends with an implicit deny statement, by design convention; there is no similar convention for route maps. If the end of a route map is reached during matching attempts, the result depends on the specific application of the route map. Fortunately, route maps that are applied to redistribution behave the same way as ACLs: if the route does not match any clause in a route map then the route redistribution is denied, as if the route map contained deny statement at the end.

The dynamic protocol **redistribute** command allows you to apply a route map. In Cisco ASDM, this capability for redistribution can be found when you add or edit a new route map (see Define a Route Map, page 21-4). Route maps are preferred if you intend to either modify route information during redistribution or if you need more powerful matching capability than an ACL can provide. If you simply need to selectively permit some routes based on their prefix or mask, we recommend that you use a route map to map to an ACL (or equivalent prefix list) directly in the **redistribute** command. If you use a route map to selectively permit some routes based on their prefix or mask, you typically use more configuration commands to achieve the same goal.

**Note**

You must use a standard ACL as the match criterion for your route map. Using an extended ACL will not work, and your routes will never be redistributed. We recommend that you number clauses in intervals of 10 to reserve numbering space in case you need to insert clauses in the future.

- Permit and Deny Clauses, page 21-2
- Match and Set Clause Values, page 21-2
- BGP Match and BGP Set Clauses, page 21-3

**Permit and Deny Clauses**

Route maps can have permit and deny clauses. In the **route-map ospf-to-eigrp** command, there is one deny clause (with sequence number 10) and two permit clauses. The deny clause rejects route matches from redistribution. Therefore, the following rules apply:

- If you use an ACL in a route map using a permit clause, routes that are permitted by the ACL are redistributed.
- If you use an ACL in a route map deny clause, routes that are permitted by the ACL are not redistributed.
- If you use an ACL in a route map permit or deny clause, and the ACL denies a route, then the route map clause match is not found and the next route-map clause is evaluated.

**Match and Set Clause Values**

Each route map clause has two types of values:

- A match value selects routes to which this clause should be applied.
- A set value modifies information that will be redistributed into the target protocol.

For each route that is being redistributed, the router first evaluates the match criteria of a clause in the route map. If the match criteria succeed, then the route is redistributed or rejected as dictated by the permit or deny clause, and some of its attributes might be modified by the values set from the Set Value tab in ASDM or from the **set** commands. If the match criteria fail, then this clause is not applicable to the route, and the software proceeds to evaluate the route against the next clause in the route map. Scanning of the route map continues until a clause is found whose **match** command(s), or Match Clause as set from the Match Clause tab in ASDM, match the route or until the end of the route map is reached.
A match or set value in each clause can be missed or repeated several times, if one of these conditions exists:

- If several **match** commands or Match Clause values in ASDM are present in a clause, all must succeed for a given route in order for that route to match the clause (in other words, the logical AND algorithm is applied for multiple match commands).

- If a **match** command or Match Clause value in ASDM refers to several objects in one command, either of them should match (the logical OR algorithm is applied). For example, in the **match ip address** 101 121 command, a route is permitted if ACL 101 or ACL 121 permits it.

- If a **match** command or Match Clause value in ASDM is not present, all routes match the clause. In the previous example, all routes that reach clause 30 match; therefore, the end of the route map is never reached.

- If a **set** command, or Set Value in ASDM, is not present in a route map permit clause, then the route is redistributed without modification of its current attributes.

---

**Note**

Do not configure a **set** command in a route map deny clause because the deny clause prohibits route redistribution—there is no information to modify.

A route map clause without a **match** or **set** command, or Match or Set Value as set on the Match or Set Value tab in ASDM, performs an action. An empty permit clause allows a redistribution of the remaining routes without modification. An empty deny clause does not allow a redistribution of other routes (this is the default action if a route map is completely scanned, but no explicit match is found).

### BGP Match and BGP Set Clauses

In addition to the match and set values described above, BGP provides additional match and set capabilities to route maps.

The following new route-map match clauses are now supported with BGP:

- match as-path
- match community
- match policy-list
- match tag

The following new route-map set clauses are now supported with BGP:

- set as-path
- set automatic-tag
- set community
- set local-preference
- set origin
- set weight

For each BGP route that is being redistributed, the ASA first evaluates the BGP match criteria of a clause in the route map. If the BGP match criteria succeeds, then the route is redistributed or rejected as dictated by the permit or deny clause, and some of its attributes might be modified by the values set from the BGP Set Clause tab in ASDM or from the **set** commands. If the match criteria fail, then this clause is not
Guidelines for Route Maps

Firewall Mode
Supported only in routed firewall mode. Transparent firewall mode is not supported.

Additional Guidelines
Route maps do not support ACLs that include a user, user group, or fully qualified domain name objects.

Define a Route Map

You must define a route map when specifying which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Procedure

Step 1 Create the route map entry:
```
route-map name {permit | deny} [sequence_number]
```

Example:
```
ciscoasa(config)# route-map name {permit} [12]
```

Route map entries are read in order. You can identify the order using the `sequence_number` argument, or the ASA uses the order in which you add route map entries.

Customize a Route Map

This section describes how to customize the route map.
- Define a Route to Match a Specific Destination Address, page 21-4
- Configure the Metric Values for a Route Action, page 21-6

Define a Route to Match a Specific Destination Address

Procedure

Step 1 Create the route map entry:
```
route-map name {permit | deny} [sequence_number]
```

Example:
ciscoasa(config)# route-map name (permit) [12]

Route map entries are read in order. You can identify the order using the sequence_number option, or the ASA uses the order in which you add route map entries.

Step 2  Match any routes that have a destination network that matches a standard ACL or prefix list:

```
match ip address acl_id [acl_id] [...] [prefix-list]
```

Example:
ciscoasa(config-route-map)# match ip address acl1

If you specify more than one ACL, then the route can match any of the ACLs.

Step 3  Match any routes that have a specified metric:

```
match metric metric_value
```

Example:
ciscoasa(config-route-map)# match metric 200

The metric_value can range from 0 to 4294967295.

Step 4  Match any routes that have a next hop router address that matches a standard ACL:

```
match ip next-hop acl_id [acl_id] [...] 
```

Example:
ciscoasa(config-route-map)# match ip next-hop acl2

If you specify more than one ACL, then the route can match any of the ACLs.

Step 5  Match any routes with the specified next hop interface:

```
match interface if_name
```

Example:
ciscoasa(config-route-map)# match interface if_name

If you specify more than one interface, then the route can match either interface.

Step 6  Match any routes that have been advertised by routers that match a standard ACL:

```
match ip route-source acl_id [acl_id] [...] 
```

Example:
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...] 

If you specify more than one ACL, then the route can match any of the ACLs.

Step 7  Match the route type:

```
match route-type {internal | external {type-1 | type-2})
```

---

Chapter 21  Route Maps

Customize a Route Map

Example:
ciscoasa(config)# route-map name (permit) [12]

Route map entries are read in order. You can identify the order using the sequence_number option, or the ASA uses the order in which you add route map entries.

Step 2  Match any routes that have a destination network that matches a standard ACL or prefix list:

```
match ip address acl_id [acl_id] [...] [prefix-list]
```

Example:
ciscoasa(config-route-map)# match ip address acl1

If you specify more than one ACL, then the route can match any of the ACLs.

Step 3  Match any routes that have a specified metric:

```
match metric metric_value
```

Example:
ciscoasa(config-route-map)# match metric 200

The metric_value can range from 0 to 4294967295.

Step 4  Match any routes that have a next hop router address that matches a standard ACL:

```
match ip next-hop acl_id [acl_id] [...] 
```

Example:
ciscoasa(config-route-map)# match ip next-hop acl2

If you specify more than one ACL, then the route can match any of the ACLs.

Step 5  Match any routes with the specified next hop interface:

```
match interface if_name
```

Example:
ciscoasa(config-route-map)# match interface if_name

If you specify more than one interface, then the route can match either interface.

Step 6  Match any routes that have been advertised by routers that match a standard ACL:

```
match ip route-source acl_id [acl_id] [...] 
```

Example:
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...] 

If you specify more than one ACL, then the route can match any of the ACLs.

Step 7  Match the route type:

```
match route-type {internal | external {type-1 | type-2})
```
Configure the Metric Values for a Route Action

If a route matches the match commands, then the following set commands determine the action to perform on the route before redistributing it.

To configure the metric value for a route action, perform the following steps:

**Procedure**

**Step 1** Create the route map entry:

```
routemap name (permit | deny) [sequence_number]
```

Example:

```
ciscoasa(config)# route-map name (permit) [12]
```

Route map entries are read in order. You can identify the order using the sequence_number argument, or the ASA uses the order in which you add route map entries.

**Step 2** Set the metric value for the route map:

```
set metric metric_value
```

Example:

```
ciscoasa(config-route-map)# set metric 200
```

The metric_value argument can range from 0 to 294967295.

**Step 3** Set the metric type for the route map:

```
set metric-type {type-1 | type-2}
```

Example:

```
ciscoasa(config-route-map)# set metric-type type-2
```

The metric-type argument can be type-1 or type-2.

Configuration Example for Route Maps

The following example shows how to redistribute routes with a hop count equal to 1 into OSPF.

The ASA redistributes these routes as external LSAs with a metric of 5 and a metric type of Type 1.

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
nciscoasa(config-route-map)# set metric 5
nciscoasa(config-route-map)# set metric-type type-1
```

The following example shows how to redistribute the 10.1.1.0 static route into eigrp process 1 with the configured metric value:

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
nciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
nciscoasa(config-route-map)# route-map mymap2 permit 10
```
Feature History for Route Maps

Table 21-1 Feature History for Route Maps

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route maps</td>
<td>7.0(1)</td>
<td>We introduced this feature. We introduced the following command: <strong>route-map</strong>.</td>
</tr>
<tr>
<td>Enhanced support for static and dynamic route maps</td>
<td>8.0(2)</td>
<td>Enhanced support for dynamic and static route maps was added.</td>
</tr>
<tr>
<td>Support for Stateful Failover of dynamic routing protocols (EIGRP, OSPF, and RIP) and debugging of general routing-related operations</td>
<td>8.4(1)</td>
<td>We introduced the following commands: <strong>debug route</strong>, <strong>show debug route</strong>. We modified the following command: <strong>show route</strong>.</td>
</tr>
<tr>
<td>Dynamic Routing in Multiple Context Mode</td>
<td>9.0(1)</td>
<td>Route maps are supported in multiple context mode.</td>
</tr>
<tr>
<td>Support for BGP</td>
<td>9.2(1)</td>
<td>We introduced this feature. We introduced the following commands: <strong>router bgp</strong>.</td>
</tr>
<tr>
<td>IPv6 support for Prefix Rule</td>
<td>9.3.2</td>
<td>We introduced this feature. We introduced the following commands:</td>
</tr>
</tbody>
</table>
BGP

This chapter describes how to configure the Cisco ASA to route data, perform authentication, and redistribute routing information using the Border Gateway Protocol (BGP).

- About BGP, page 22-1
- Guidelines for BGP, page 22-3
- Configure BGP, page 22-4
- Monitoring BGP, page 22-30
- Configuration Example for BGP, page 22-32
- History for BGP, page 22-34

About BGP

BGP is an inter autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

- When to Use BGP, page 22-1
- Routing Table Changes, page 22-2

When to Use BGP

Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

Note

BGP can now be used for carrying routing information for IPv6 prefix over IPv6 networks. When a BGPv6 ASA joins the cluster, it generates a soft traceback when logging level 7 is enabled.
Routing Table Changes

BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and BGP routing updates advertise only the optimal path to a destination network.

Routes learned via BGP have properties that are used to determine the best route to a destination, when multiple paths exist to a particular destination. These properties are referred to as BGP attributes and are used in the route selection process:

- Weight -- This is a Cisco-defined attribute that is local to a router. The weight attribute is not advertised to neighboring routers. If the router learns about more than one route to the same destination, the route with the highest weight is preferred.

- Local preference -- The local preference attribute is used to select an exit point from the local AS. Unlike the weight attribute, the local preference attribute is propagated throughout the local AS. If there are multiple exit points from the AS, the exit point with the highest local preference attribute is used as an exit point for a specific route.

- Multi-exit discriminator -- The multi-exit discriminator (MED) or metric attribute is used as a suggestion to an external AS regarding the preferred route into the AS that is advertising the metric. It is referred to as a suggestion because the external AS that is receiving the MEDs may also be using other BGP attributes for route selection. The route with the lower MED metric is preferred.

- Origin -- The origin attribute indicates how BGP learned about a particular route. The origin attribute can have one of three possible values and is used in route selection.
  - IGP- The route is interior to the originating AS. This value is set when the network router configuration command is used to inject the route into BGP.
  - EGP-The route is learned via the Exterior Border Gateway Protocol (EBGP).
  - Incomplete- The origin of the route is unknown or learned in some other way. An origin of incomplete occurs when a route is redistributed into BGP.

- AS_path -- When a route advertisement passes through an autonomous system, the AS number is added to an ordered list of AS numbers that the route advertisement has traversed. Only the route with the shortest AS_path list is installed in the IP routing table.

- Next hop -- The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS.

- Community -- The community attribute provides a way of grouping destinations, called communities, to which routing decisions (such as acceptance, preference, and redistribution) can be applied. Route maps are used to set the community attribute. The predefined community attributes are as follows:
  - no-export- Do not advertise this route to EBGP peers.
  - no-advertise- Do not advertise this route to any peer.
  - internet- Advertise this route to the Internet community; all routers in the network belong to it.
BGP Path Selection

BGP may receive multiple advertisements for the same route from different sources. BGP selects only one path as the best path. When this path is selected, BGP puts the selected path in the IP routing table and propagates the path to its neighbors. BGP uses the following criteria, in the order presented, to select a path for a destination:

- If the path specifies a next hop that is inaccessible, drop the update.
- Prefer the path with the largest weight.
- If the weights are the same, prefer the path with the largest local preference.
- If the local preferences are the same, prefer the path that was originated by BGP running on this router.
- If no route was originated, prefer the route that has the shortest AS_path.
- If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than incomplete).
- If the origin codes are the same, prefer the path with the lowest MED attribute.
- If the paths have the same MED, prefer the external path over the internal path.
- If the paths are still the same, prefer the path through the closest IGP neighbor.
- If both paths are external, prefer the path that was received first (the oldest one).
- Prefer the path with the lowest IP address, as specified by the BGP router ID.
- If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length.
- Prefer the path that comes from the lowest neighbor address.

Guidelines for BGP

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Does not support transparent firewall mode. BGP is supported only in router mode.

Failover Guidelines

Supports Stateful Failover in single and multiple context mode.

Note

When clustering is enabled, failover is not supported.

Clustering Guidelines

BGP is supported only in L2 (EtherChannel Type) and L3 (Individual Interface Type) clustering modes.

Note

When you delete and reapply the BGP configuration in the user context allow a delay of 60 seconds, to enable the slave/standby ASA unit to sync.
IPv6 Guidelines
Supports IPv6. Graceful restart is not supported for IPv6 address family.

Configure BGP

This section describes how to enable and configure the BGP process on your system.

Procedure

Step 1  In the CLI, enable BGP, and configure general BGP parameters.

Step 2  Define the best path for the BGP routing process and configure the best path configuration parameters.

Step 3  Add and configure policy lists.

Step 4  Add and configure AS path filters.

Step 5  Add and configure Community Rules.

Step 6  Configure IPv4 Address Family settings.

Enable BGP

This section describes the steps required to enable BGP routing, establish a BGP routing process and configure general BGP parameters.

Procedure

Step 1  Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:
```
ciscoasa(config)# router bgp 2
```

Valid values for `autonomous-num` are from 1-4294967295 and 1.0-XX.YY.

Step 2  Discard routes that have as-path segments that exceed a specified value:

```
bgp maxas-limit number
```

Example:
```
ciscoasa(config-router)# bgp maxas-limit 15
```

The `number` argument specifies the maximum number of autonomous system segments, allowed. Valid values are from 1 to 254.

Step 3  Log BGP neighbor resets:

```
bgp log-neighbor-changes
```

Step 4  Enable BGP to automatically discover the best TCP path MTU for each BGP session:

```
bgp transport path-mtu-discovery
```
Step 5 Enable BGP to terminate external BGP sessions of any directly adjacent peer if the link used to reach the peer goes down; without waiting for the hold-down timer to expire:

```
bgp fast-external-fallover
```

Step 6 Allow a BGP routing process to discard updates received from an external BGP (eBGP) peers that do not list their autonomous system (AS) number as the first AS path segment in the AS_PATH attribute of the incoming route:

```
bgp enforce-first-as
```

Step 7 Change the default display and regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation:

```
bgp asnotation dot
```

Step 8 Adjust BGP network timers:

```
timers bgp keepalive holdtime [min-holdtime]
```

Example:

```
ciscoasa(config-router)# timers bgp 80 120
```

- `keepalive` — frequency (in seconds) with which the ASA sends keepalive messages to its peer. The default value is 60 seconds.
- `holdtime` — interval (in seconds) after not receiving a keepalive message that the ASA declares a peer dead. The default is 180 seconds.
- (Optional) `min-holdtime` — interval (in seconds) after not receiving a keepalive message from a neighbor, that the ASA declares a neighbor dead.

Step 9 Enables BGP graceful restart capability:

```
bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]
```

Example:

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- `restart-time` — maximum time period (in seconds) that the ASA will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default is 120 seconds. Valid values are from 1 to 3600 seconds.
- `stalepath-time` — maximum time period (in seconds) that the ASA will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value is 360 seconds. Valid values are from 1 to 3600 seconds.

---

**Define the Best Path for a BGP Routing Process**

This section describes the steps required to configure the BGP best path. For more information on the best path, see BGP Path Selection, page 22-3.

**Procedure**

**Step 1** Enable a BGP routing process, which places the ASA in router configuration mode:
**Configure BGP**

```
router bgp autonomous-num
```

Example:
ciscoasa(config)# router bgp 2

**Step 2** Change the default local preference value:
```
bgp default local-preference number
```

Example:
ciscoasa(config-router)# bgp default local-preference 500

The `number` argument is any value between 0 and 4294967295. Higher values indicate higher preference. The default value is 100.

**Step 3** Enable Multi Exit Discriminator (MED) comparison among paths learned from neighbors in different autonomous systems:
```
bgp always-compare-med
```

**Step 4** Compare between similar routes received from external BGP (eBGP) peers during the best path selection process and switch the best path to the route with the lowest router ID:
```
bgp bestpath compare-routerid
```

**Step 5** Select the best MED path advertised from the neighboring AS:
```
bgp deterministic-med
```

**Step 6** Set a path with a missing MED attribute as the least preferred path:
```
bgp bestpath med missing-as-worst
```

---

**Configure Policy Lists**

When a policy list is referenced within a route map, all of the match statements within the policy list are evaluated and processed. Two or more policy lists can be configured with a route map. A policy list can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy list. This section describes the steps required to configure policy lists.

**Procedure**

**Step 1** Enable the policy-map configuration mode and allows you to create a BGP policy list:
```
policy-list policy_list_name {permit | deny}
```

Example:
ciscoasa(config)# policy-list Example-policy-list1 permit

The `permit` keyword allows access for matching conditions.
The `deny` keyword denies access for matching conditions.

**Step 2** Distribute routes that have their next hop out one of the interfaces specified:
```
match interface [...interface_name]
```
Example:
ciscoasa(config-policy-list)# match interface outside

Step 3  Redistribute routes by matching either or all of the following: the destination address, next hop router address, and router/access server source:
match ip (address | next-hop | route-source)

Step 4  Match a BGP autonomous system path:
macth as-path

Step 5  Match a BGP community:
macth community (community-list_name | exact-match)
Example:
ciscoasa(config-policy-list)# match community ExampleCommunity1
  • community-list_name — one or more community lists.
  • exact-match — indicates that an exact match is required. All of the communities and only those communities specified must be present.

Step 6  Redistribute routes with the metric specified:
macth metric

Step 7  Redistribute routes in the routing table that match the specified tags:
macth tag

Configure AS Path Filters

An AS path filter allows you to filter the routing update message by using access lists and look at the individual prefixes within an update message. If a prefix within the update message matches the filter criteria then that individual prefix is filtered out or accepted depending on what action the filter entry has been configured to carry out. This section describes the steps required to configure AS path filters.

Note
The as-path access-lists are not the same as the regular firewall ACLs.

Procedure

Step 1  Configure an autonomous system path filter using a regular expression in the global configuration mode:
as-path access-list acl-number (permit|deny) regexp

Example:
ciscoasa(config)# as-path access-list 35 permit testaspath
  • acl-number — AS-path access-list number. Valid values are from 1 to 500.
Configure Community Rules

A community is a group of destinations that share some common attribute. You can use community lists to create groups of communities to use in a match clause of a route map. Just like an access list, a series of community lists can be created. Statements are checked until a match is found. As soon as one statement is satisfied, the test is concluded. This section describes the steps required to configure community rules.

**Procedure**

**Step 1** Create or configure a BGP community list and control access to it:

```
community-list {standard | community list-name (deny|permit) [community-number] [AA:NN] [internet] [no-advertise][no-export]) | {expanded | expanded list-name (deny|permit) regexp}
```

Example:

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise no-export
```

- **standard** — configures a standard community list using a number from 1 to 99 to identify one or more permit or deny groups of communities.
- **(Optional) community-number** — community as a 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.
- **AA:NN** — an autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered for each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.
- **(Optional) internet** — specifies the Internet community. Routes with this community are advertised to all peers (internal and external).
- **(Optional) no-advertise** — specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).
- **(Optional) no-export** — specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.
- **(Optional) expanded** — configures an expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.
- **regexp** — regular expression that defines the AS-path filter. The autonomous system number is expressed in the range from 1 to 65535.

**Note** Regular expressions can be used only with expanded community lists.
Configure IPv4 Address Family Settings

The IPv4 settings for BGP can be set up from the IPv4 family option within the BGP configuration setup. The IPv4 family section includes subsections for General settings, Aggregate address settings, Filtering settings and Neighbor settings. Each of these subsections enable you to customize parameters specific to the IPv4 family.

This section describes how to customize the BGP IPv4 family settings.

- Configure IPv4 Family General Settings, page 22-9
- Configure IPv4 Family Aggregate Address Settings, page 22-11
- Configure IPv4 Family Filtering Settings, page 22-12
- Configure IPv4 Family BGP Neighbor Settings, page 22-13
- Configure IPv4 Network Settings, page 22-18
- Configure Redistribution Settings, page 22-18
- Configure Route Injection Settings, page 22-19

Configure IPv4 Family General Settings

This section describes the steps required to configure the general IPv4 settings.

Procedure

- **Step 1** Enable a BGP routing process, which places the router in router configuration mode:

  `router bgp autonomous-num`

  Example:

  `ciscoasa(config)# router bgp 2`

- **Step 2** Enter address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes:

  `address-family ipv4 {unicast}`

  The keyword `unicast` specifies IPv4 unicast address prefixes. This is the default, even if not specified.

- **Step 3** (Optional) Configure a fixed router ID for the local BGP routing process:

  `bgp router-id A.B.C.D`

  Example:

  `ciscoasa(config-router-af)# bgp router-id 10.86.118.3`

  The argument `A.B.C.D` specifies a router identifier in the form of an IP address. If you do not specify a router ID, it is automatically assigned.

- **Step 4** (Optional) Configure a cluster pool of IP addresses in the Individual Interface (L3) mode:

  `bgp router-id cluster-pool`

  Example:

  `ciscoasa(config-router-af)# bgp router-id cp`
Configure BGP

Note: In an L3 cluster, you cannot define a BGP neighbor as one of the cluster pool IP addresses.

Step 5  Configure the administrative distance for BGP routes:

```
distance bgp external-distance internal-distance local-distance
```

Example:

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- `external-distance` — administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
- `internal-distance` — administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
- `local-distance` — administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.

Step 6  Modify metric and tag values when the IP routing table is updated with BGP learned routes:

```
table-map {WORD|route-map_name}
```

Example:

```
ciscoasa(config-router-af)# table-map example1
```

The argument `route-map_name` specifies the route map name from the `route-map` command.

Step 7  Configure a BGP routing process to distribute a default route (network 0.0.0.0):

```
default-information originate
```

Step 8  Configure automatic summarization of subnet routes into network-level routes:

```
auto-summary
```

Step 9  Suppress the advertisement of routes that are not installed in the routing information base (RIB):

```
bgp suppress-inactive
```

Step 10  Synchronize between BGP and your Interior Gateway Protocol (IGP) system:

```
synchronization
```

Step 11  Configure iBGP redistribution into an IGP, such as OSPF:

```
bgp redistribute-internal
```

Step 12  Configure scanning intervals of BGP routers for next hop validation:

```
bgp scan-time scanner-interval
```

Example:

```
ciscoasa(config-router-af)# bgp scan-time 15
```
The argument *scanner-interval* specifies scanning interval of BGP routing information. Valid values are from 5 to 60 seconds. The default is 60 seconds.

**Step 13** Configure BGP next-hop address tracking:

```
bgp nexthop trigger \{delay seconds\|enable\}
```

Example:
```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- **trigger** — specifies the use of BGP next-hop address tracking. Use this keyword with the **delay** keyword to change the next-hop tracking delay. Use this keyword with the **enable** keyword to enable next-hop address tracking.
- **delay** — changes the delay interval between checks on updated next-hop routes installed in the routing table.
- **seconds** — specifies the delay in seconds. Range is from 0 to 100. Default is 5.
- **enable** — enables BGP next-hop address tracking immediately.

**Step 14** Control the maximum number of parallel iBGP routes that can be installed in a routing table:

```
maximum-paths \{number_of_paths|ibgp number_of_paths\}
```

Example:
```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

The **number_of_paths** argument specifies the number of routes to install to the routing table. In ASA 9.3(1), valid values are between 1 and 3. In ASA 9.3(2) and later, valid values are between 1 and 8.

**Note** If the **ibgp** keyword is not used, then the **number_of_paths** argument controls the maximum number of parallel EBGP routes.

---

**Configure IPv4 Family Aggregate Address Settings**

This section describes the steps required to define the aggregation of specific routes into one route.

**Procedure**

**Step 1** Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:
```
ciscoasa(config)# router bgp 2
```

**Step 2** Enter address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes:

```
address-family ipv4 \{unicast\}
```

The keyword **unicast** specifies IPv4 unicast address prefixes. This is the default, even if not specified.
Configure BGP

Step 3 Create an aggregate entry in a BGP database:

```
aggregate-address address mask [as-set] [summary-only] [suppress-map map-name] [advertise-map map-name] [attribute-map map-name]
```

Example:

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only suppress-map example1 advertise-map example1 attribute-map example1
```

- **address** — the aggregate address.
- **mask** — the aggregate mask.
- **map-name** — the route map.
- **as-set** — (Optional) generates autonomous system set path information.
- **summary-only** — (Optional) filters all more-specific routes from updates.
- **Suppress-map map-name** — (Optional) specifies the name of the route map used to select the routes to be suppressed.
- **Advertise-map map-name** — (Optional) specifies the name of the route map used to select the routes to create AS_SET origin communities.
- **Attribute-map map-name** — (Optional) specifies the name of the route map used to set the attribute of the aggregate route.

Configure IPv4 Family Filtering Settings

This section describes the steps required to filter routes or networks received in incoming BGP updates.

Procedure

**Step 1** Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:

```
ciscoasa(config)# router bgp 2
```

**Step 2** Enter address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes:

```
address-family ipv4 [unicast]
```

The keyword **unicast** specifies IPv4 unicast address prefixes. This is the default, even if not specified.

**Step 3** Filter routes or networks received in incoming or advertised in outgoing BGP updates:

```
distribute-list acl-number in|out
```

Example:

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

The argument **acl-number** specifies IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
Configure BGP

The keyword **in** specifies that the filter must be applied to incoming BGP updates and **out** specifies that the filter must be applied to outgoing BGP updates.

## Configure IPv4 Family BGP Neighbor Settings

This section describes the steps required to define BGP neighbors and neighbor settings.

**Procedure**

**Step 1** Enable a BGP routing process, which places the router in router configuration mode:

```
router bgp autonomous-num
```

Example:

```
ciscoasa(config)# router bgp 2
```

**Step 2** Enter address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes:

```
address-family ipv4 [unicast]
```

The keyword **unicast** specifies IPv4 unicast address prefixes. This is the default, even if not specified.

**Step 3** Add an entry to the BGP neighbor table:

```
neighbor ip-address remote-as autonomous-number
```

Example:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

**Step 4** (Optional) Disable a neighbor or peer group:

```
neighbor ip-address shutdown
```

Example:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

**Step 5** Exchange information with a BGP neighbor:

```
neighbor ip-address activate
```

Example:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

**Step 6** Enable or disable the Border Gateway Protocol (BGP) graceful restart capability for a BGP neighbor:

```
neighbor ip-address ha-mode graceful-restart [disable]
```

Example:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

(Optional) The **disable** keyword disables BGP graceful restart capability for a neighbor.

**Step 7** Distribute BGP neighbor information as specified in an access list:

```
neighbor (ip-address) distribute-list {access-list-name}{in|out}
```

Example:
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in

- `access-list-number` — the number of a standard or extended access list. The range of a standard access list number is from 1 to 99. The range of an extended access list number is from 100 to 199.
- `expanded-list-number` — the number of an expanded access list number. The range of an expanded access list is from 1300 to 2699.
- `access-list-name` — the name of a standard or extended access list.
- `prefix-list-name` — the name of a BGP prefix list.
- `in` — that the access list is applied to incoming advertisements to that neighbor.
- `out` — that the access list is applied to outgoing advertisements to that neighbor.

Step 8  Apply a route map to incoming or outgoing routes:
```
neighbor {ip-address} route-map map-name {in|out}
```

Example:
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in

The keyword **in** applies a route map to incoming routes.
The keyword **out** applies a route map to outgoing routes.

Step 9  Distribute BGP neighbor information as specified in a prefix list:
```
neighbor {ip-address} prefix-list prefix-list-name {in|out}
```

Example:
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in

The keyword **in** implies that the prefix list is applied to incoming advertisements from that neighbor.
The keyword **out** implies that the prefix list is applied to outgoing advertisements to that neighbor.

Step 10  Set up a filter list:
```
neighbor {ip-address} filter-list access-list-number {in|out}
```

Example:
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in

- `access-list-name` — specifies the number of an autonomous system path access list. You define this access list with the `ip as-path access-list` command.
- `in` — that the access list is applied to incoming advertisements from that neighbor.
- `out` — that the access list is applied to outgoing advertisements to that neighbor.

Step 11  Control the number of prefixes that can be received from a neighbor:
```
neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]
```

Example:
Configure BGP

Step 12 Allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route:
```
neighbor (ip-address) default-originate [route-map map-name]
```
Example:
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1

The argument map-name is the name of the route-map. The route map allows route 0.0.0.0 to be injected conditionally.

Step 13 Set the minimum interval between the sending of BGP routing updates:
```
neighbor (ip-address) advertisement-interval seconds
```
Example:
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15

The argument seconds is the time (in seconds). Valid values are from 0 to 600.

Step 14 Advertise the routes in the BGP table that matches the configured route-map:
```
neighbor (ip-address) advertise-map map-name [exist-map map-name | non-exist-map map-name] [check-all-paths]
```
Example:
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2

- **advertise-map map name** — the name of the route map that will be advertised if the conditions of the exist map or non-exist map are met.
- **exist-map map name** — the name of the exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
- **non-exist-map map name** — the name of the non-exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
- (Optional) **check all paths** — enables checking of all paths by the exist-map with a prefix in the BGP table.

Step 15 Remove private autonomous system numbers from outbound routing updates:
```
neighbor (ip-address) remove-private-as
```
Example:
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as

Step 16 Sets the timers for a specific BGP peer or peer group.
```
neighbor (ip-address) timers keepalive holdtime min holdtime
```

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```
- **maximum** — the maximum number of prefixes allowed from this neighbor.
- (Optional) **threshold** — integer specifying at what percentage of maximum the router starts to generate a warning message. The range is from 1 to 100; the default is 75 (percent).
- (Optional) **restart interval** — integer value (in minutes) that specifies the time interval after which the BGP neighbor restarts.
- (Optional) **warning-only** — allows the router to generate a log message when the maximum number of prefixes is exceeded, instead of terminating the peering.
Example:
```cisco
Ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- **keepalive** — the frequency (in seconds) with which the ASA sends keepalive messages to its peer. The default is 60 seconds. Valid values are from 0 to 65535.
- **holdtime** — the interval (in seconds) after not receiving a keepalive message that the ASA declares a peer dead. The default is 180 seconds.
- **min holdtime** — the minimum interval (in seconds) after not receiving a keepalive message that the ASA declares a peer dead.

**Step 17**
Enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers:
```
neighbor (ip-address) password string
```

Example:
```cisco
Ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

The argument `string` is a case-sensitive password of up to 25 characters when the `service password-encryption` command is enabled and up to 81 characters when the `service password-encryption` command is not enabled. The string can contain any alphanumeric characters, including spaces.

**Note**
The first character cannot be a number. You cannot specify a password in the format number-space-anything. The space after the number can cause authentication to fail.

**Step 18**
Specify that communities attributes should be sent to a BGP neighbor:
```
neighbor (ip-address) send-community [both | standard | extended]
```

Example:
```cisco
Ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

- (Optional) **both** keyword — both standard and extended communities will be sent.
- (Optional) **standard** keyword — only standard communities will be sent.
- (Optional) **extended** keyword — only extended communities will be sent.

**Step 19**
Configure the router as the next hop for a BGP-speaking neighbor or peer group:
```
neighbor (ip-address) next-hop-self
```

Example:
```cisco
Ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

**Step 20**
Accept and attempt BGP connections to external peers residing on networks that are not directly connected:
```
neighbor (ip-address) ebgp-multihop [ttl]
```

Example:
```cisco
Ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

The argument `ttl` specifies time-to-live in the range from 1 to 255 hops.
**Step 21** Disable connection verification to establish an eBGP peering session with a single-hop peer that uses a loopback interface:

```plaintext
eighbor (ip-address) disable-connected-check
```

Example:
```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

**Step 22** Secure a BGP peering session and configures the maximum number of hops that separate two external BGP (eBGP) peers:

```plaintext
neighbor (ip-address) ttl-security hops hop-count
```

Example:
```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

The argument `hop-count` is the number of hops that separate the eBGP peers. The TTL value is calculated by the router from the configured hop-count argument. Valid values are from 1 to 254.

**Step 23** Assign a weight to a neighbor connection:

```plaintext
neighbor (ip-address) weight number
```

Example:
```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

The argument `number` is the weight to assign to a neighbor connection. Valid values are from 0 to 65535.

**Step 24** Configure the ASA to accept only a particular BGP version:

```plaintext
neighbor (ip-address) version number
```

Example:
```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

The argument `number` specifies the BGP version number. The version can be set to 2 to force the software to use only Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

**Step 25** Enable a TCP transport session option for a BGP session:

```plaintext
neighbor (ip-address) transport {connection-mode (active|passive)| path-mtu-discovery {disable}}
```

Example:
```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- `connection-mode` — the type of connection (active or passive).
- `path-mtu-discovery` — enables TCP transport path maximum transmission unit (MTU) discovery. TCP path MTU discovery is enabled by default.
- (Optional) `disable` — disables TCP path MTU discovery.

**Step 26** Customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor:

```plaintext
neighbor (ip-address) local-as {autonomous-system-number|no-prepend|replace-as}
```

Example:
```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```
Configure BGP

(Optional) autonomous-system-number — the number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 4294967295 or 1.0 to XX.YY.

(Optional) no-prepend — does not prepend the local autonomous system number to any routes received from the eBGP neighbor.

Configure IPv4 Network Settings

This section describes the steps required to define the networks to be advertised by the BGP routing process.

Procedure

Step 1 Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:

```
ciscoasa(config)# router bgp 2
```

Step 2 Enter address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes:

```
address-family ipv4 [unicast]
```

The keyword unicast specifies IPv4 unicast address prefixes. This is the default, even if not specified.

Step 3 Specify the networks to be advertised by the BGP routing processes:

```
network {network-number [mask network-mask]}[route-map map-tag]
```

Example:

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

- network-number — the network that BGP will advertise.
- (Optional) network-mask — the network or subnetwork mask with mask address.
- (Optional) map-tag — the identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised.

Configure Redistribution Settings

This section describes the steps required to define the conditions for redistributing routes from another routing domain into BGP.

Procedure

Step 1 Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:
Configure BGP

Step 2  Enter address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes:

address-family ipv4 [unicast]

Example:

ciscoasa(config-router)# address-family ipv4[unicast]

The keyword unicast specifies IPv4 unicast address prefixes. This is the default, even if not specified.

Step 3  Redistribute routes from another routing domain into a BGP autonomous system:

redistribute protocol [process-id] [metric] [route-map [map-tag]]

Example:

ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external

- protocol — the source protocol from which routes are being redistributed. It can be one of the following: Connected, EIGRP, OSPF, RIP or Static.
- (Optional) process-id — a name for the specific routing process.
- (Optional) metric — the metric for the redistributed route.
- (Optional) map-tag — the identifier of a configured route map.

Note  The route map should be examined to filter the networks to be redistributed. If not specified, all networks are redistributed.

Configure Route Injection Settings

This section describes the steps required to define the routes to be conditionally injected into the BGP routing table.

Procedure

Step 1  Enable a BGP routing process, which places the ASA in router configuration mode:

router bgp autonomous-num

Example:

ciscoasa(config)# router bgp 2

Step 2  Enter address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes:

address-family ipv4 [unicast]

Example:

ciscoasa(config-router)# address-family ipv4[unicast]

The keyword unicast specifies IPv4 unicast address prefixes. This is the default, even if not specified.

Step 3  Configure conditional route injection to inject more specific routes into a BGP routing table:
configure bgp

bgp inject-map inject-map exist-map exist-map [copy-attributes]

Example:

ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes

- *inject-map* — the name of the route map that specifies the prefixes to inject into the local BGP routing table.
- *exist-map* — the name of the route map containing the prefixes that the BGP speaker will track.
- (Optional) *copy-attributes* — configures the injected route to inherit attributes of the aggregate route.

Configure IPv6 Address Family Settings

The IPv6 settings for BGP can be set up from the IPv6 family option within the BGP configuration setup. The IPv6 family section includes subsections for General settings, Aggregate address settings and Neighbor settings. Each of these subsections enable you to customize parameters specific to the IPv6 family.

This section describes how to customize the BGP IPv6 family settings.

- Configure IPv6 Family General Settings, page 22-20
- Configure IPv6 Family Aggregate Address Settings, page 22-21
- Configure IPv6 Family BGP Neighbor Settings, page 22-22
- Configure IPv6 Network Settings, page 22-27
- Configure Redistribution Settings, page 22-18
- Configure Route Injection Settings, page 22-19

Configure IPv6 Family General Settings

This section describes the steps required to configure the general IPv6 settings.

Procedure

**Step 1** Enable a BGP routing process, which places the router in router configuration mode:

```
router bgp autonomous-num
```

Example:

ciscoasa(config)# router bgp 2

**Step 2** Enter address family configuration mode to configure a routing session using standard IP Version 6 (IPv6) address prefixes:

```
address-family ipv6 [unicast]
```

**Step 3** Configure the administrative distance for BGP routes:

```
distance bgp external-distance internal-distance local-distance
```
Example:
```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- **external-distance** — administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
- **internal-distance** — administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
- **local-distance** — administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.

**Step 4** (Optional) Configure a BGP routing process to distribute a default route (network 0.0.0.0):
```
default-information originate
```

**Step 5** (Optional) Suppress the advertisement of routes that are not installed in the routing information base (RIB):
```
bgp suppress-inactive
```

**Step 6** Synchronize between BGP and your Interior Gateway Protocol (IGP) system:
```
synchronization
```

**Step 7** Configure iBGP redistribution into an IGP, such as OSPF:
```
bgp redistribute-internal
```

**Step 8** Configure scanning intervals of BGP routers for next hop validation:
```
bgp scan-time scanner-interval
```
Example:
```
ciscoasa(config-router-af)# bgp scan-time 15
```
Valid values for the *scanner-interval* argument from 5 to 60 seconds. The default is 60 seconds.

**Step 9** Control the maximum number of parallel iBGP routes that can be installed in a routing table:
```
maximum-paths {number_of_paths|ibgp number_of_paths}
```
Example:
```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```
Valid values for the *number_of_paths* argument is between 1 and 8.
If the *ibgp* keyword is not used, then the *number_of_paths* argument controls the maximum number of parallel EBGP routes.

---

**Configure IPv6 Family Aggregate Address Settings**

This section describes the steps required to define the aggregation of specific routes into one route.
**Configure BGP**

**Procedure**

**Step 1**  
Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:

```
ciscoasa(config)# router bgp 2
```

**Step 2**  
Enter address family configuration mode to configure a routing session using standard IP Version 6 (IPv6) address prefixes:

```
address-family ipv6 unicast
```

**Step 3**  
Create an aggregate entry in a BGP database:

```
aggregate-address ipv6-address/cidr [as-set] [summary-only] [suppress-map map-name] [advertise-map ipv6-map-name] [attribute-map map-name]
```

Example:

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- **address** — the aggregate IPv6 address.
- (Optional) **as-set** — generates autonomous system set path information.
- (Optional) **summary-only** — filters all more-specific routes from updates.
- (Optional) **suppress-map map-name** — specifies the name of the route map used to select the routes to be suppressed.
- (Optional) **advertise-map map-name** — specifies the name of the route map used to select the routes to create AS_SET origin communities.
- (Optional) **attribute-map map-name** — specifies the name of the route map used to set the attribute of the aggregate route.

**Step 4**  
Set the interval at which BGP routes will be aggregated:

```
bgp aggregate-timer seconds
```

Example:

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

---

**Configure IPv6 Family BGP Neighbor Settings**

This section describes the steps required to define BGP neighbors and neighbor settings.

**Procedure**

**Step 1**  
Enable a BGP routing process, which places the router in router configuration mode:

```
router bgp autonomous-num
```

Example:

```
ciscoasa(config)# router bgp 2
```
Step 2 Enter address family configuration mode to configure a routing session using standard IP Version 6 (IPv6) address prefixes:

```
address-family ipv6 [unicast]
```

Step 3 Add an entry to the BGP neighbor table:

```
neighbor ipv6-address remote-as autonomous-number
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

The argument `ipv6-address` specifies the IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. When an interface type and interface number are specified, you can optionally specify the IPv6 address of the next hop to which packets are output. You must specify an interface type and an interface number when using a link-local address as the next hop (the link-local next hop must also be an adjacent device).

*Note* This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Step 4 (Optional) Disable a neighbor or peer group:

```
neighbor ipv6-address shutdown
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

Step 5 Exchange information with a BGP neighbor:

```
neighbor ipv6-address activate
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

Step 6 Apply a route map to incoming or outgoing routes:

```
neighbor (ipv6-address) route-map map-name {in|out}
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

The keyword `in` applies a route map to incoming routes.
The keyword `out` applies a route map to outgoing routes.

Step 7 Distribute BGP neighbor information as specified in a prefix list:

```
neighbor (ipv6-address) prefix-list prefix-list-name {in|out}
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

The keyword `in` implies that the prefix list is applied to incoming advertisements from that neighbor.
The keyword `out` implies that the prefix list is applied to outgoing advertisements to that neighbor.
Step 8  Set up a filter list:

```
neighbor (ipv6-address) filter-list access-list-name {in|out}
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```
- `access-list-name` — specifies the number of an autonomous system path access list. You define this access list with the `ip as-path access-list` command.
- `in` — that the access list is applied to incoming advertisements from that neighbor.
- `out` — that the access list is applied to outgoing advertisements to that neighbor.

Step 9  Control the number of prefixes that can be received from a neighbor:

```
neighbor (ipv6-address) maximum-prefix maximum [threshold] [restart restart interval] [warning-only]
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```
- `maximum` — the maximum number of prefixes allowed from this neighbor.
- (Optional) `threshold` — integer specifying at what percentage of maximum the router starts to generate a warning message. The range is from 1 to 100; the default is 75 (percent).
- (Optional) `restart interval` — integer value (in minutes) that specifies the time interval after which the BGP neighbor restarts.
- (Optional) `warning-only` — allows the router to generate a log message when the maximum number of prefixes is exceeded, instead of terminating the peering.

Step 10  Allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route:

```
neighbor (ipv6-address) default-originate [route-map map-name]
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```
The argument `map-name` is the name of the route-map. The route map allows route 0.0.0.0 to be injected conditionally.

Step 11  Set the minimum interval between the sending of BGP routing updates:

```
neighbor (ipv6-address) advertisement-interval seconds
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```
The argument `seconds` is the time (in seconds). Valid values are from 0 to 600.

Step 12  Remove private autonomous system numbers from outbound routing updates:

```
neighbor (ipv6-address) remove-private-as
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

Step 13  Advertise the routes in the BGP table that matches the configured route-map:

```
neighbor (ipv6-address) advertise-map map-name {exist-map map-name | non-exist-map map-name} [check-all-paths]
```
Example:
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2

- **advertise-map** *map name* — the name of the route map that will be advertised if the conditions of the exist map or non-exist map are met.
- **exist-map** *map name* — the name of the exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
- **non-exist-map** *map name* — the name of the non-exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
- (Optional) **check all paths** — enables checking of all paths by the exist-map with a prefix in the BGP table.

**Step 14** Sets the timers for a specific BGP peer or peer group.

```
neighbor (ipv6-address) timers keepalive holdtime min holdtime
```

Example:
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12

- **keepalive** — the frequency (in seconds) with which the ASA sends keepalive messages to its peer. The default is 60 seconds. Valid values are from 0 to 65535.
- **holdtime** — the interval (in seconds) after not receiving a keepalive message that the ASA declares a peer dead. The default is 180 seconds.
- **min holdtime** — the minimum interval (in seconds) after not receiving a keepalive message that the ASA declares a peer dead.

**Step 15** Enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers:

```
neighbor (ipv6-address) password string
```

Example:
ciscoasa(config-router-af)# neighbor 2000::1 password test

The argument *string* is a case-sensitive password of up to 25 characters when the **service password-encryption** command is enabled and up to 81 characters when the **service password-encryption** command is not enabled. The string can contain any alphanumeric characters, including spaces.

**Note**
The first character cannot be a number. You cannot specify a password in the format number-space-anything. The space after the number can cause authentication to fail.

**Step 16** Specify that communities attributes should be sent to a BGP neighbor:

```
neighbor (ipv6-address) send-community [standard]
```

Example:
ciscoasa(config-router-af)# neighbor 2000::1 send-community

- (Optional) **standard** keyword — only standard communities will be sent.

**Step 17** Configure the router as the next hop for a BGP-speaking neighbor or peer group:

```
neighbor (ipv6-address) next-hop-self
```

---

Cisco ASA Series General Operations CLI Configuration Guide  22-25
Configure BGP

Step 18
Accept and attempt BGP connections to external peers residing on networks that are not directly connected:

```
neighbor (ipv6-address) ebgp-multihop [ttl]
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

The argument `ttl` specifies time-to-live in the range from 1 to 255 hops.

Step 19
Disable connection verification to establish an eBGP peering session with a single-hop peer that uses a loopback interface:

```
neighbor (ipv6-address) disable-connected-check
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

Step 20
Secure a BGP peering session and configures the maximum number of hops that separate two external BGP (eBGP) peers:

```
neighbor (ipv6-address) ttl-security hops hop-count
```

Example:
```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

The argument `hop-count` is the number of hops that separate the eBGP peers. The TTL value is calculated by the router from the configured hop-count argument. Valid values are from 1 to 254.

Step 21
Assign a weight to a neighbor connection:

```
neighbor (ipv6-address) weight number
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

The argument `number` is the weight to assign to a neighbor connection. Valid values are from 0 to 65535.

Step 22
Configure the ASA to accept only a particular BGP version:

```
neighbor (ipv6-address) version number
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

The argument `number` specifies the BGP version number. The default is Version 4. Currently only BGP version 4 is supported.

Step 23
Enable a TCP transport session option for a BGP session:

```
neighbor (ipv6-address) transport {connection-mode|active|passive} | path-mtu-discovery|disable}
```

Example:
```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- `connection-mode` — the type of connection (`active` or `passive`).

---

**Cisco ASA Series General Operations CLI Configuration Guide**
Configure BGP

Step 24

Customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor:

```
neighbor (ipv6-address) local-as [autonomous-system-number[no-prepend]]
```

Example:

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (Optional) `autonomous-system-number` — the number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 4294967295 or 1.0 to XX.YY.
- (Optional) `no-prepend` — does not prepend the local autonomous system number to any routes received from the eBGP neighbor.

Caution

BGP prepends the autonomous system number from each BGP network that a route traverses to maintain network reachability information and to prevent routing loops. This command should be configured only for autonomous system migration, and should be removed after the transition has been completed. This procedure should be attempted only by an experienced network operator. Routing loops can be created through improper configuration.

Configure IPv6 Network Settings

This section describes the steps required to define the networks to be advertised by the BGP routing process.

Procedure

Step 1

Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:

```
ciscoasa(config)# router bgp 2
```

Step 2

Enter address family configuration mode to configure a routing session using standard IP Version 6 (IPv6) address prefixes:

```
address-family ipv6 [unicast]
```

Step 3

Specify the networks to be advertised by the BGP routing processes:

```
network (ipv6 network/ prefix length) [route-map route-map name]
```

Example:

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
```

- `ipv6 network/prefix length`— the network that BGP will advertise.
Configure BGP

(Optional) `route-map name` — the identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised.

Configure Redistribution Settings

This section describes the steps required to define the conditions for redistributing routes from another routing domain into BGP.

Procedure

**Step 1**
Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:
```
ciscoasa(config)# router bgp 2
```

**Step 2**
Enter address family configuration mode to configure a routing session using standard IP Version 6 (IPv6) address prefixes:

```
address-family ipv6 [unicast]
```

Example:
```
ciscoasa(config-router)# address-family ipv6[unicast]
```

**Step 3**
Redistribute routes from another routing domain into a BGP autonomous system:

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|external|external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]] [subnets]
```

Example:
```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- `protocol` — the source protocol from which routes are being redistributed. It can be one of the following: Connected, EIGRP, OSPF, RIP or Static.
- (Optional) `process-id` — For the ospf protocol, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number.

**Note**
This value is auto-populated for the other protocols.

- (Optional) metric `metric value` — When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified. The default value is 0.
- (Optional) match `internal|external|external1|external2|NSSA external 1|NSSA external 2` — For the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following:
  - `internal` — Routes that are internal to a specific autonomous system.
  - `external` — Routes that are external to the autonomous system, but are imported into BGP as OSPF Type 1 external route.
Configure BGP

- **external 2** — Routes that are external to the autonomous system, but are imported into BGP as OSPF Type 2 external route.
- **NSSA external 1** — Routes that are external to the autonomous system, but are imported into BGP as OSPF NSSA Type 1 external route.
- **NSSA external 2** — Routes that are external to the autonomous system, but are imported into BGP as OSPF NSSA Type 2 external route.
- *(Optional)* **map-tag** — the identifier of a configured route map.

**Note**
The route map should be examined to filter the networks to be redistributed. If not specified, all networks are redistributed.

**Configure Route Injection Settings**

This section describes the steps required to define the routes to be conditionally injected into the BGP routing table.

**Procedure**

**Step 1**
Enable a BGP routing process, which places the ASA in router configuration mode:

```
router bgp autonomous-num
```

Example:
```
ciscoasa(config)# router bgp 2
```

**Step 2**
Enter address family configuration mode to configure a routing session using standard IP Version 6 (IPv6) address prefixes:

```
address-family ipv6 [unicast]
```

Example:
```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

**Step 3**
Configure conditional route injection to inject more specific routes into a BGP routing table:

```
bgp inject-map inject-map exist-map exist-map [copy-attributes]
```

Example:
```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- **inject-map** — the name of the route map that specifies the prefixes to inject into the local BGP routing table.
- **exist-map** — the name of the route map containing the prefixes that the BGP speaker will track.
- *(Optional)* **copy-attributes** — configures the injected route to inherit attributes of the aggregate route.
Monitoring BGP

You can use the following commands to monitor the BGP routing process. For examples and descriptions of the command output, see the command reference. Additionally, you can disable the logging of neighbor change messages and neighbor warning messages.

To monitor various BGP routing statistics, enter one of the following commands:

- **show bgp [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]] | prefix-list name | route-map name]**
  Displays the entries in the BGP routing table.

- **show bgp cidr-only**
  Displays routes with non-natural network masks (that is, classless interdomain routing, or CIDR).

- **show bgp community community-number [exact-match][no-advertise][no-export]**
  Display routes that belong to specified BGP communities.

- **show bgp community-list community-list-name [exact-match]**
  Displays routes that are permitted by the BGP community list.

- **show bgp filter-list access-list-number**
  Displays routes that conform to a specified filter list.

- **show bgp injected-paths**
  Displays all the injected paths in the BGP routing table.

- **show bgp ipv4 unicast**
  Displays entries in the IP version 4 (IPv4) BGP routing table for unicast sessions.

- **show bgp ipv6 unicast**
  Displays entries in the IPv6 Border Gateway Protocol (BGP) routing table.

- **show bgp ipv6 community**
  Displays routes that belong to specified IPv6 Border Gateway Protocol (BGP) communities.

- **show bgp ipv6 community-list**
  Displays routes that are permitted by the IPv6 Border Gateway Protocol (BGP) community list.

- **show bgp ipv6 filter-list**
  Display routes that conform to a specified IPv6 filter list.

- **show bgp ipv6 inconsistent-as**
  Displays IPv6 Border Gateway Protocol (BGP) routes with inconsistent originating autonomous systems.

- **show bgp ipv6 neighbors**
  Displays information about IPv6 Border Gateway Protocol (BGP) connections to neighbors.

- **show bgp ipv6 paths**
  Displays all the IPv6 Border Gateway Protocol (BGP) paths in the database.

- **show bgp ipv6 prefix-list**
  Displays routes that match a prefix list.

- **show bgp ipv6 quote-regexp**
Chapter 22      BGP

Monitoring BGP

Displays IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression as a quoted string of characters.

- **show bgp ipv6 regexp**
  Displays IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression.

- **show bgp ipv6 route-map**
  Displays IPv6 Border Gateway Protocol (BGP) routes that failed to install in the routing table.

- **show bgp ipv6 summary**
  Displays the status of all IPv6 Border Gateway Protocol (BGP) connections.

- **show bgp neighbors ip_address**
  Displays information about BGP and TCP connections to neighbors.

- **show bgp paths** [LINE]
  Displays all the BGP paths in the database.

- **show bgp pending-prefixes**
  Displays prefixes that are pending deletion.

- **show bgp prefix-list prefix_list_name [WORD]**
  Displays routes that match a specified prefix list.

- **show bgp regexp regexp**
  Displays routes that match the autonomous system path regular expression.

- **show bgp replication [index-group | ip-address]**
  Displays update replication statistics for BGP update groups.

- **show bgp rib-failure**
  Displays BGP routes that failed to install in the Routing Information Base (RIB) table.

- **show bgp route-map map-name**
  Displays entries in the BGP routing table, based on the route map specified.

- **show bgp summary**
  Display the status of all BGP connections.

- **show bgp system-config**
  Display the system context specific BGP configuration in multi-context mode.
  This command is available in all user contexts in multi-context mode.

- **show bgp update-group**
  Display information about the BGP update groups.

---

To disable BGP Log messages, enter the **no bgp log-neighbor-changes** command in the router configuration mode. This disables the logging of neighbor change messages. Enter this command in router configuration mode for the BGP routing process. By default, neighbor changes are logged.
Configuration Example for BGP

This example shows how to enable and configure BGPv4 with various optional processes.

Step 1 Define the conditions for redistributing routes from one routing protocol into another, or enable policy routing:
```
ciscoasa(config)# route-map mymap2 permit 10
```

Step 2 Redistribute any routes that have a route address or match packet that is passed by one of the access lists specified:
```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

Step 3 Indicate where to output packets that pass a match clause of a route map for policy routing:
```
ciscoasa(config-route-map)# set ip next-hop peer address
```

Step 4 Enable a BGP routing process from the global configuration mode:
```
ciscoasa(config)# router bgp 2
```

Step 5 Configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process in the address family configuration mode:
```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

Step 6 Add an entry to the BGP neighbor table:
```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

Step 7 Apply a route map to incoming or outgoing routes:
```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

This example shows how to enable and configure BGPv6 with various optional processes.

Step 1 Define the conditions for redistributing routes from one routing protocol into another, or enable policy routing:
```
ciscoasa(config)# route-map mymap1 permit 10
```

Step 2 Redistribute any routes that have a route address or match packet that is passed by one of the access lists specified:
```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

Step 3 Indicate where to output packets that pass a match clause of a route map for policy routing:
```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

Step 4 Enable a BGP routing process from the global configuration mode:
```
ciscoasa(config)# router bgp 2
```

Step 5 Configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process in the address family configuration mode:
```
ciscoasa(config)# address-family ipv4
```
ciscoasa(config-router-af)# bgp router-id 19.168.254.254

**Step 6** Enter address family configuration mode to configure a routing session using standard IP Version 6 (IPv6) address prefixes:
address-family ipv6 [unicast]

**Step 7** Add an entry to the BGP neighbor table:
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600

**Step 8** Apply a route map to incoming or outgoing routes:
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
# History for BGP

Table 22-1 lists each feature change and the platform release in which it was implemented.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Support</td>
<td>9.2(1)</td>
<td>Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the Border Gateway Protocol. We introduced the following commands: <code>router bgp</code>, <code>bgp maxas-limit</code>, <code>bgp log-neighbor-changes</code>, <code>bgp transport path-mtu-discovery</code>, <code>bgp fast-external-fallover</code>, <code>bgp enforce-first-as</code>, <code>bgp asnotation dot</code>, <code>timers bgp</code>, <code>bgp default local-preference</code>, <code>bgp always-compare-med</code>, <code>bgp bestpath compare-routerid</code>, <code>bgp deterministic-med</code>, <code>bgp bestpath med missing-as-worst</code>, <code>policy-list</code>, <code>match as-path</code>, <code>match community</code>, <code>match metric</code>, <code>match tag</code>, <code>as-path access-list</code>, <code>community-list</code>, <code>address-family ipv4</code>, <code>bgp router-id</code>, <code>distance bgp</code>, <code>table-map</code>, <code>bgp suppress-inactive</code>, <code>bgp redistribute-internal</code>, <code>bgp scan-time</code>, <code>bgp nexthop</code>, <code>aggregate-address</code>, <code>neighbor</code>, <code>bgp inject-map</code>, <code>show bgp</code>, <code>show bgp cidr-only</code>, <code>show bgp all community</code>, <code>show bgp all neighbors</code>, <code>show bgp community</code>, <code>show bgp community-list</code>, <code>show bgp filter-list</code>, <code>show bgp injected-paths</code>, <code>show bgp ipv4 unicast</code>, <code>show bgp neighbors</code>, <code>show bgp paths</code>, <code>show bgp pending-prefixes</code>, <code>show bgp prefix-list</code>, <code>show bgp regexp</code>, <code>show bgp replication</code>, <code>show bgp rib-failure</code>, <code>show bgp route-map</code>, <code>show bgp summary</code>, <code>show bgp system-config</code>, <code>show bgp update-group</code>, <code>clear route network</code>, <code>maximum-path</code>, <code>network</code>.</td>
</tr>
<tr>
<td>BGP support for ASA clustering</td>
<td>9.3(1)</td>
<td>We added support for L2 and L3 clustering. We introduced the following new command: <code>bgp router-id clusterpool</code></td>
</tr>
</tbody>
</table>
### Table 22-1 Feature History for BGP

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP support for nonstop forwarding</td>
<td>9.3(1)</td>
<td>We added support for Nonstop Forwarding. We introduced the following new commands: <code>bgp graceful-restart</code>, <code>neighbor ha-mode graceful-restart</code></td>
</tr>
<tr>
<td>BGP support for advertised maps</td>
<td>9.3(1)</td>
<td>We added support for BGPv4 advertised map. We introduced the following new command: <code>neighbor advertise-map</code></td>
</tr>
<tr>
<td>BGP support for IPv6</td>
<td>9.3(2)</td>
<td>We added support for IPv6. We introduced the following new commands: <code>address-family ipv6</code>, <code>ipv6 prefix-list</code>, <code>ipv6 prefix-list description</code>, <code>ipv6 prefix-list sequence-number</code>, <code>match ipv6 next-hop</code>, <code>match ipv6 route-source</code>, <code>match ipv6 address prefix-list</code>, <code>set ipv6-address prefix-list</code>, <code>set ipv6 next-hop</code>, <code>set ipv6 next-hop peer-address</code> We modified the following command: <code>bgp router-id</code></td>
</tr>
</tbody>
</table>
This chapter describes how to configure the Cisco ASA to route data, perform authentication, and redistribute routing information using the Open Shortest Path First (OSPF) routing protocol.

The chapter includes the following sections:

- About OSPF, page 23-1
- Guidelines for OSPF, page 23-4
- Configure OSPFv2, page 23-6
- Configure OSPF Fast Hello Packets, page 23-7
- Customize OSPFv2, page 23-7
- Configure OSPFv3, page 23-18
- Configure Graceful Restart, page 23-37
- Example for OSPFv2, page 23-41
- Examples for OSPFv3, page 23-43
- Monitoring OSPF, page 23-44
- Additional References, page 23-47
- History for OSPF, page 23-47

### About OSPF

OSPF is an interior gateway routing protocol that uses link states rather than distance vectors for path selection. OSPF propagates link-state advertisements rather than routing table updates. Because only LSAs are exchanged instead of the entire routing tables, OSPF networks converge more quickly than RIP networks.

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

The advantages of OSPF over RIP include the following:

- OSPF link-state database updates are sent less frequently than RIP updates, and the link-state database is updated instantly, rather than gradually, as stale information is timed out.
• Routing decisions are based on cost, which is an indication of the overhead required to send packets across a certain interface. The ASA calculates the cost of an interface based on link bandwidth rather than the number of hops to the destination. The cost can be configured to specify preferred paths.

The disadvantage of shortest path first algorithms is that they require a lot of CPU cycles and memory. The ASA can run two processes of OSPF protocol simultaneously on different sets of interfaces. You might want to run two processes if you have interfaces that use the same IP addresses (NAT allows these interfaces to coexist, but OSPF does not allow overlapping addresses). Or you might want to run one process on the inside and another on the outside, and redistribute a subset of routes between the two processes. Similarly, you might need to segregate private addresses from public addresses.

You can redistribute routes into an OSPF routing process from another OSPF routing process, a RIP routing process, or from static and connected routes configured on OSPF-enabled interfaces.

The ASA supports the following OSPF features:

• Intra-area, interarea, and external (Type I and Type II) routes.
• Virtual links.
• LSA flooding.
• Authentication to OSPF packets (both password and MD5 authentication).
• Configuring the ASA as a designated router or a designated backup router. The ASA also can be set up as an ABR.
• Stub areas and not-so-stubby areas.
• Area boundary router Type 3 LSA filtering.

OSPF supports MD5 and clear text neighbor authentication. Authentication should be used with all routing protocols when possible because route redistribution between OSPF and other protocols (such as RIP) can potentially be used by attackers to subvert routing information.

If NAT is used, if OSPF is operating on public and private areas, and if address filtering is required, then you need to run two OSPF processes—one process for the public areas and one for the private areas.

A router that has interfaces in multiple areas is called an Area Border Router (ABR). A router that acts as a gateway to redistribute traffic between routers using OSPF and routers using other routing protocols is called an Autonomous System Boundary Router (ASBR).

An ABR uses LSAs to send information about available routes to other OSPF routers. Using ABR Type 3 LSA filtering, you can have separate private and public areas with the ASA acting as an ABR. Type 3 LSAs (interarea routes) can be filtered from one area to other, which allows you to use NAT and OSPF together without advertising private networks.

Only Type 3 LSAs can be filtered. If you configure the ASA as an ASBR in a private network, it will send Type 5 LSAs describing private networks, which will get flooded to the entire AS, including public areas.

If NAT is employed but OSPF is only running in public areas, then routes to public networks can be redistributed inside the private network, either as default or Type 5 AS external LSAs. However, you need to configure static routes for the private networks protected by the ASA. Also, you should not mix public and private networks on the same ASA interface.

You can have two OSPF routing processes, one RIP routing process, and one EIGRP routing process running on the ASA at the same time.
**OSPF Support for Fast Hello Packets**

The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than 1 second. Such a configuration would result in faster convergence in an Open Shortest Path First (OSPF) network.

**Prerequisites for OSPF Support for Fast Hello Packets**

OSPF must be configured in the network already or configured at the same time as the OSPF Support for Fast Hello Packets feature.

**Information About OSPF Support for Fast Hello Packets**

The following sections describe concepts related to OSPF support for fast hello packets:

- OSPF Hello Interval and Dead Interval
- OSPF Fast Hello Packets
- Benefits of OSPF Fast Hello Packets

**OSPF Hello Interval and Dead Interval**

OSPF hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The defaults are 10 seconds for an Ethernet link and 30 seconds for a non broadcast link. Hello packets include a list of all neighbors for which a hello packet has been received within the dead interval. The dead interval is also a configurable interval (in seconds), and defaults to four times the value of the hello interval. The value of all hello intervals must be the same within a network. Likewise, the value of all dead intervals must be the same within a network.

These two intervals work together to maintain connectivity by indicating that the link is operational. If a router does not receive a hello packet from a neighbor within the dead interval, it will declare that neighbor to be down.

**OSPF Fast Hello Packets**

OSPF fast hello packets refer to hello packets being sent at intervals of less than 1 second. To understand fast hello packets, you should already understand the relationship between OSPF hello packets and the dead interval. See OSPF Hello Interval and Dead Interval, page 23-3.

OSPF fast hello packets are achieved by using the `ospf dead-interval` command. The dead interval is set to 1 second, and the hello-multiplier value is set to the number of hello packets you want sent during that 1 second, thus providing subsecond or “fast” hello packets.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.
Benefits of OSPF Fast Hello Packets

The benefit of the OSPF Fast Hello Packets feature is that your OSPF network will experience faster convergence time than it would without fast hello packets. This feature allows you to detect lost neighbors within 1 second. It is especially useful in LAN segments, where neighbor loss might not be detected by the Open System Interconnection (OSI) physical layer and data-link layer.

Implementation Differences Between OSPFv2 and OSPFv3

OSPFv3 is not backward compatible with OSPFv2. To use OSPF to route both IPv4 and IPv6 traffic, you must run both OSPFv2 and OSPFv3 at the same time. They coexist with each other, but do not interact with each other.

The additional features that OSPFv3 provides include the following:

- Protocol processing per link.
- Removal of addressing semantics.
- Addition of flooding scope.
- Support for multiple instances per link.
- Use of the IPv6 link-local address for neighbor discovery and other features.
- LSAs expressed as prefix and prefix length.
- Addition of two LSA types.
- Handling of unknown LSA types.
- Authentication support using the IPsec ESP standard for OSPFv3 routing protocol traffic, as specified by RFC-4552.

Guidelines for OSPF

Context Mode Guidelines
OSPFv2 supports single and multiple context mode.
OSPFv3 supports single mode only.

Firewall Mode Guidelines
OSPF supports routed firewall mode only. OSPF does not support transparent firewall mode.

Failover Guidelines
OSPFv2 and OSPFv3 support Stateful Failover.

IPv6 Guidelines
- OSPFv2 does not support IPv6.
- OSPFv3 supports IPv6.
- OSPFv3 uses IPv6 for authentication.
- The ASA installs OSPFv3 routes into the IPv6 RIB, provided it is the best route.
- OSPFv3 packets can be filtered out using IPv6 ACLs in the capture command.
Guidelines for OSPF

Clustering Guidelines

- OSPFv2 and OSPFv3 support clustering.
- OSPFv3 encryption is not supported. An error message appears if you try to configure OSPFv3 encryption in a clustering environment.
- In the spanned interface mode, dynamic routing is not supported on management-only interfaces.
- In individual interface mode, make sure that you establish the master and slave units as either OSPFv2 or OSPFv3 neighbors.
- When you configure both OSPFv2 and EIGRP, you can use either spanned interface mode or individual interface mode; you cannot use the two modes at the same time.
- In individual interface mode, 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.
- The router ID is optional in the OSPFv2, OSPFv3, and EIGRP router configuration mode. If you do not explicitly set a router ID, then a router ID is automatically generated and set to the highest IPv4 address on any data interface in each of the cluster units.
- If the cluster interface mode has not been configured, then only a single, dotted-decimal IPv4 address is allowed as the router ID, and the cluster pool option is disabled.
- If the cluster interface mode is set to a spanned configuration, then only a single, dotted-decimal IPv4 address is allowed as the router ID, and the cluster pool option is disabled.
- If the cluster interface mode is set to an individual configuration, then the cluster pool option is mandatory, and a single, dotted-decimal IPv4 address is not allowed as the router ID.
- When the cluster interface mode is changed from a spanned to an individual configuration and vice versa without specifying the check-detail or nocheck options, then the entire configuration including the router ID is removed.
- If any of the dynamic routing protocol router ID configurations are incompatible with the new interface mode, then an error message appears on the console and the interface mode CLI fails. The error message has one line per dynamic routing protocol (OSPFv2, OSPFv3, and EIGRP) and lists the names of each context in which the incompatible configuration occurs.
- If the nocheck option is specified for the cluster interface mode command, then the interface mode is allowed to change although all the router ID configurations may not be compatible with the new mode.
- When the cluster is enabled, the router ID compatibility checks are repeated. If any incompatibility is detected, then the cluster enable command fails. The administrator needs to correct the incompatible router ID configuration before the cluster can be enabled.
- When a unit enters a cluster as a slave, then we recommend that you specify the nocheck option for the cluster interface mode command to avoid any router ID compatibility check failures. The slave unit still inherits the router configuration from the master unit.
- When a mastership role change occurs in the cluster, the following behavior occurs:
  - In spanned interface mode, the router process is active only on the master unit and is in a suspended state on the slave units. Each cluster unit has the same router ID because the configuration has been synchronized from the master unit. As a result, a neighboring router does not notice any change in the router ID of the cluster during a role change.
  - In individual interface mode, the router process is active on all the individual cluster units. Each cluster unit chooses its own distinct router ID from the configured cluster pool. A mastership role change in the cluster does not change the routing topology in any way.
Additional Guidelines

- OSPFv2 and OSPFv3 support multiple instances on an interface.
- OSPFv3 supports encryption through ESP headers in a non-clustered environment.
- OSPFv3 supports Non-Payload Encryption.
- OSPFv2 supports Cisco NSF Graceful Restart and IETF NSF Graceful Restart mechanisms as defined in RFCs 4811, 4812 & 3623 respectively.
- OSPFv3 supports Graceful Restart mechanism as defined in RFC 5187.

Configure OSPFv2

This section describes how to enable an OSPFv2 process on the ASA.

After you enable OSPFv2, you need to define a route map. For more information, see Define a Route Map, page 21-4. Then you generate a default route. For more information, see Configure a Static Route, page 20-4.

After you have defined a route map for the OSPFv2 process, you can customize it for your particular needs. To learn how to customize the OSPFv2 process on the ASA, see Customize OSPFv2, page 23-7.

To enable OSPFv2, you need to create an OSPFv2 routing process, specify the range of IP addresses associated with the routing process, then assign area IDs associated with that range of IP addresses.

You can enable up to two OSPFv2 process instances. Each OSPFv2 process has its own associated areas and networks.

To enable OSPFv2, perform the following steps:

Procedure

---

**Step 1** Create an OSPF routing process:

`router ospf process_id`

Example:

```
ciscoasa(config)# router ospf 2
```

The `process_id` argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

If there is only one OSPF process enabled on the ASA, then that process is selected by default. You cannot change the OSPF process ID when editing an existing area.

**Step 2** Define the IP addresses on which OSPF runs and the area ID for that interface:

`network ip_address mask area area_id`

Example:

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```
When adding a new area, enter the area ID. You can specify the area ID as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295. You cannot change the area ID when editing an existing area.

---

**Configure OSPF Fast Hello Packets**

This section describes how to configure OSPF Fast Hello Packets.

**Procedure**

**Step 1** Configure an interface:
```
interface port-channel number
```
Example:
```
ciscoasa(config)# interface port-channel 10
```
The *number* argument indicates the port-channel interface number.

**Step 2** Set the interval during which at least one hello packet must be received, or else the neighbor is considered down:
```
ospf dead-interval minimal hello-multiplier no.of times
```
Example:
```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
ciscoasa
```
The *no. of times* argument indicates the number of hello packets to be sent every second. Valid values are between 3 and 20.

In this example, OSPF Support for Fast Hello Packets is enabled by specifying the minimal keyword and the hello-multiplier keyword and value. Because the multiplier is set to 5, five hello packets will be sent every second.

---

**Customize OSPFv2**

This section explains how to customize the OSPFv2 processes.

- Redistribute Routes Into OSPFv2, page 23-8
- Configure Route Summarization When Redistributing Routes Into OSPFv2, page 23-9
- Configure Route Summarization Between OSPFv2 Areas, page 23-10
- Configure OSPFv2 Interface Parameters, page 23-11
- Configure OSPFv2 Area Parameters, page 23-14
- Configure an OSPFv2 NSSA, page 23-15
Redistribute Routes Into OSPFv2

The ASA can control the redistribution of routes between OSPFv2 routing processes.

If you want to redistribute a route by defining which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process, you must first generate a default route. See Configure a Static Route, page 20-4, and then define a route map according to Define a Route Map, page 21-4.

To redistribute static, connected, RIP, or OSPFv2 routes into an OSPFv2 process, perform the following steps:

Procedure

Step 1  Create an OSPF routing process:

\[ \text{router ospf process_id} \]

Example:

ciscoasa(config)# router ospf 2

The \textit{process_id} argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

Step 2  Redistribute connected routes into the OSPF routing process:

\[ \text{redistribute connected} \ [\text{metric metric-value} \ [\text{metric-type} \ {\text{type-1} \ | \ \text{type-2}}]] \ [\text{tag tag-value}] \ [\text{subnets}] \ [\text{route-map map_name}] \]

Example:

ciscoasa(config)# redistribute connected 5 type-1 route-map-practice

Step 3  Redistribute static routes into the OSPF routing process:

\[ \text{redistribute static} \ [\text{metric metric-value} \ [\text{metric-type} \ {\text{type-1} \ | \ \text{type-2}}]] \ [\text{tag tag-value}]
 \ [\text{subnets}] \ [\text{route-map map_name}] \]

Example:

ciscoasa(config)# redistribute static 5 type-1 route-map-practice

Step 4  Redistribute routes from an OSPF routing process into another OSPF routing process:

\[ \text{redistribute ospf pid} \ [\text{match} \ {\text{internal} \ | \ \text{external} \ [1 \ | \ 2] \ | \ \text{nssa-external} \ [1 \ | \ 2]}] \ [\text{metric metric-value} \ [\text{metric-type} \ {\text{type-1} \ | \ \text{type-2}}]] \ [\text{tag tag-value}] \ [\text{subnets}] \ [\text{route-map map_name}] \]

Example:

ciscoasa(config)# redistribute ospf 1 [match internal] 1 type-1 route-map-practice
Chapter 23      OSPF

Customize OSPFv2

Example:

ciscoasa(config)# route-map 1-to-2 permit
  ciscoasa(config-route-map)# match metric 1
  ciscoasa(config-route-map)# set metric 5
  ciscoasa(config-route-map)# set metric-type type-1
  ciscoasa(config-route-map)# router ospf 2
  ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2

You can either use the match options in this command to match and set route properties, or you can use a route map. The subnets option does not have equivalents in the route-map command. If you use both a route map and match options in the redistribute command, then they must match.

The example shows route redistribution from OSPF process 1 into OSPF process 2 by matching routes with a metric equal to 1. The ASA redistributes these routes as external LSAs with a metric of 5 and a metric type of Type 1.

Step 5  Redistribute routes from a RIP routing process into the OSPF routing process:

redistribute rip [metric metric-value] [metric-type {type-1 | type-2}] [tag tag_value] [subnets] [route-map map_name]

Example:

ciscoasa(config)# redistribute rip 5
  ciscoasa(config-route-map)# match metric 1
  ciscoasa(config-route-map)# set metric 5
  ciscoasa(config-route-map)# set metric-type type-1
  ciscoasa(config-route-map)# redistribute ospf 1 route-map 1-to-2

Step 6  Redistribute routes from an EIGRP routing process into the OSPF routing process:

redistribute eigrp as-num [metric metric-value] [metric-type {type-1 | type-2}] [tag tag_value] [subnets] [route-map map_name]

Example:

ciscoasa(config)# redistribute eigrp 2
  ciscoasa(config-route-map)# match metric 1
  ciscoasa(config-route-map)# set metric 5
  ciscoasa(config-route-map)# set metric-type type-1
  ciscoasa(config-route-map)# redistribute ospf 1 route-map 1-to-2

Configure Route Summarization When Redistributing Routes Into OSPFv2

When routes from other protocols are redistributed into OSPF, each route is advertised individually in an external LSA. However, you can configure the ASA to advertise a single route for all the redistributed routes that are included for a specified network address and mask. This configuration decreases the size of the OSPF link-state database.

Routes that match the specified IP address mask pair can be suppressed. The tag value can be used as a match value for controlling redistribution through route maps.

To configure route summarization, you can:

• Add a Route Summary Address, page 23-10
Add a Route Summary Address

To configure the software advertisement on one summary route for all redistributed routes included for a network address and mask, perform the following steps:

Procedure

Step 1  Create an OSPF routing process:
         
         \text{router ospf process\_id}

         Example:
         ciscoasa(config)# router ospf 1

         The \text{process\_id} argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

Step 2  Set the summary address:
         \text{summary-address ip\_address mask [not-advertise] [tag tag]}

         Example:
         ciscoasa(config)# router ospf 1
         ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0

         In this example, the summary address 10.1.0.0 includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the 10.1.0.0 address is advertised in an external link-state advertisement.

Configure Route Summarization Between OSPFv2 Areas

Route summarization is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an area boundary router. In OSPF, an area boundary router advertises networks in one area into another area. If the network numbers in an area are assigned in a way so that they are contiguous, you can configure the area boundary router to advertise a summary route that includes all the individual networks within the area that fall into the specified range.

To define an address range for route summarization, perform the following steps:

Procedure

Step 1  Create an OSPF routing process and enters router configuration mode for this OSPF process:
         \text{router ospf process\_id}
Example:
ciscoasa(config)# router ospf 1
The \textit{process\_id} argument is an internally used identifier for this routing process. It can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

\textbf{Step 2} Set the address range:

\texttt{area area-id range ip-address mask [advertise | not-advertise]}

Example:
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0

In this example, the address range is set between OSPF areas.

\section*{Configure OSPFv2 Interface Parameters}

You can change some interface-specific OSPFv2 parameters, if necessary. You are not required to change any of these parameters, but the following interface parameters must be consistent across all routers in an attached network: \texttt{ospf hello-interval}, \texttt{ospf dead-interval}, and \texttt{ospf authentication-key}. If you configure any of these parameters, be sure that the configurations for all routers on your network have compatible values.

To configure OSPFv2 interface parameters, perform the following steps:

\textbf{Procedure}

\textbf{Step 1} Create an OSPF routing process:

\texttt{router ospf process\_id}

Example:
ciscoasa(config)# router ospf 2

The \textit{process\_id} argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

\textbf{Step 2} Define the IP addresses on which OSPF runs and the area ID for that interface:

\texttt{network ip-address mask area area_id}

Example:
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0

\textbf{Step 3} Enter interface configuration mode:

\texttt{interface interface\_name}

Example:
ciscoasa(config)# interface my\_interface
**Step 4** Specify the authentication type for an interface:

```
ospf authentication [message-digest | null]
```

Example:
```
ciscoasa(config-interface)# ospf authentication message-digest
```

**Step 5** Assign a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication:

```
ospf authentication-key key
```

Example:
```
ciscoasa(config-interface)# ospf authentication-key cisco
```

The `key` argument can be any continuous string of characters up to 8 bytes in length.

The password created by this command is used as a key that is inserted directly into the OSPF header when the ASA software originates routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

**Step 6** Explicitly specify the cost of sending a packet on an OSPF interface:

```
ospf cost cost
```

Example:
```
ciscoasa(config-interface)# ospf cost 20
```

The `cost` is an integer from 1 to 65535.

In this example, the cost is set to 20.

**Step 7** Set the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet:

```
ospf dead-interval seconds
```

Example:
```
ciscoasa(config-interface)# ospf dead-interval 40
```

The value must be the same for all nodes on the network.

**Step 8** Specify the length of time between the hello packets that the ASA sends on an OSPF interface:

```
ospf hello-interval seconds
```

Example:
```
ciscoasa(config-interface)# ospf hello-interval 10
```

The value must be the same for all nodes on the network.

**Step 9** Enable OSPF MD5 authentication:

```
ospf message-digest-key key_id md5 key
```

Example:
```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

The following argument values can be set:
Key_id—an identifier in the range from 1 to 255.

Key—an alphanumeric password of up to 16 bytes.

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

Step 10 Set the priority to help determine the OSPF designated router for a network:

```
ospf priority number_value
```

Example:

```
ciscoasa(config-interface)# ospf priority 20
```

The `number_value` argument ranges from 0 to 255.

Step 11 Specify the number of seconds between LSA retransmissions for adjacencies belonging to an OSPF interface:

```
ospf retransmit-interval seconds
```

Example:

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

The value for `seconds` must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 8192 seconds. The default value is 5 seconds.

Step 12 Set the estimated number of seconds required to send a link-state update packet on an OSPF interface:

```
ospf transmit-delay seconds
```

Example:

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

The `seconds` value ranges from 1 to 8192 seconds. The default value is 1 second.

Step 13 Set the number of hello packets sent during 1 second:

```
ospf dead-interval minimal hello-interval multiplier
```

Example:

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

Valid values are integers between 3 and 20.

Step 14 Specify the interface as a point-to-point, non-broadcast network:

```
ospf network point-to-point non-broadcast
```

Example:

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```
When you designate an interface as point-to-point and non-broadcast, you must manually define the OSPF neighbor; dynamic neighbor discovery is not possible. See Define Static OSPFv2 Neighbors, page 23-16 for more information. Additionally, you can only define one OSPF neighbor on that interface.

Configure OSPFv2 Area Parameters

You can configure several OSPF area parameters. These area parameters (shown in the following task list) include setting authentication, defining stub areas, and assigning specific costs to the default summary route. Authentication provides password-based protection against unauthorized access to an area.

Stub areas are areas into which information on external routes is not sent. Instead, there is a default external route generated by the ABR into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, default routing must be used in the stub area. To further reduce the number of LSAs sent into a stub area, you can use the **no-summary** keyword of the **area stub** command on the ABR to prevent it from sending a summary link advertisement (LSA Type 3) into the stub area.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create an OSPF routing process:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>router ospf process_id</strong></td>
</tr>
</tbody>
</table>

Example:

ciscoasa(config)# router ospf 2

The *process_id* argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Enable authentication for an OSPF area:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>area area-id authentication</strong></td>
</tr>
</tbody>
</table>

Example:

ciscoasa(config-rtr)# area 0 authentication

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Enable MD5 authentication for an OSPF area:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>area area-id authentication message-digest</strong></td>
</tr>
</tbody>
</table>

Example:

ciscoasa(config-rtr)# area 0 authentication message-digest
Configure an OSPFv2 NSSA

The OSPFv2 implementation of an NSSA is similar to an OSPFv2 stub area. NSSA does not flood Type 5 external LSAs from the core into the area, but it can import autonomous system external routes in a limited way within the area.

NSSA imports Type 7 autonomous system external routes within an NSSA area by redistribution. These Type 7 LSAs are translated into Type 5 LSAs by NSSA ABRs, which are flooded throughout the whole routing domain. Summarization and filtering are supported during the translation.

You can simplify administration if you are an ISP or a network administrator that must connect a central site using OSPFv2 to a remote site that is using a different routing protocol with NSSA.

Before the implementation of NSSA, the connection between the corporate site border router and the remote router could not be run as an OSPFv2 stub area because routes for the remote site could not be redistributed into the stub area, and two routing protocols needed to be maintained. A simple protocol such as RIP was usually run and handled the redistribution. With NSSA, you can extend OSPFv2 to cover the remote connection by defining the area between the corporate router and the remote router as an NSSA.

Before you use this feature, consider these guidelines:
- You can set a Type 7 default route that can be used to reach external destinations. When configured, the router generates a Type 7 default into the NSSA or the NSSA area boundary router.
- Every router within the same area must agree that the area is NSSA; otherwise, the routers cannot communicate with each other.

Procedure

**Step 1**
Create an OSPF routing process:

```
router ospf process_id
```

Example:
```
ciscoasa(config)# router ospf 2
```

The `process_id` argument is an internally used identifier for this routing process. It can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

**Step 2**
Define an NSSA area:

```
area area-id nssa [no-redistribution] [default-information-originate]
```

Example:
```
ciscoasa(config-rtr)# area 0 nssa
```

**Step 3**
Set the summary address and helps reduce the size of the routing table:

```
summary-address ip_address mask [not-advertise] [tag tag]
```

Example:
```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

Using this command for OSPF causes an OSPF ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by the address.
In this example, the summary address 10.1.0.0 includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the 10.1.0.0 address is advertised in an external link-state advertisement.

Note: OSPF does not support summary-address 0.0.0.0 0.0.0.0.

### Configure an IP Address Pool for Clustering (OSPFv2 and OSPFv3)

You can assign a range of IPv4 addresses for the router ID cluster pool if you are using Individual Interface clustering.

**Procedure**

To assign a range of IPv4 addresses for the router ID cluster pool in Individual Interface clustering for OSPFv2 and OSPFv3, enter the following command:

**Step 1** Specify the router ID cluster pool for Individual Interface clustering:

```
router-id cluster-pool hostname | A.B.C.D ip_pool
```

Example:

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

The **cluster-pool** keyword enables configuration of an IP address pool when Individual Interface clustering is configured. The **hostname | A.B.C.D** keyword specifies the OSPF router ID for this OSPF process. The **ip_pool** argument specifies the name of the IP address pool.

Note: If you are using clustering, then you do not need to specify an IP address pool for the router ID. If you do not configure an IP address pool, then the ASA uses the automatically generated router ID.

### Define Static OSPFv2 Neighbors

You need to define static OSPFv2 neighbors to advertise OSPFv2 routes over a point-to-point, non-broadcast network. This feature lets you broadcast OSPFv2 advertisements across an existing VPN connection without having to encapsulate the advertisements in a GRE tunnel.

Before you begin, you must create a static route to the OSPFv2 neighbor. See Chapter 20, “Static and Default Routes,” for more information about creating static routes.
Chapter 23      OSPF

Customize OSPFv2

Procedure

Step 1  Create an OSPFv2 routing process:
router ospf process_id

Example:
ciscoasa(config)# router ospf 2

The process_id argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

Step 2  Define the OSPFv2 neighborhood:
neighbor addr [interface if_name]

Example:
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]

The addr argument is the IP address of the OSPFv2 neighbor. The if_name argument is the interface used to communicate with the neighbor. If the OSPFv2 neighbor is not on the same network as any of the directly connected interfaces, you must specify the interface.

Configure Route Calculation Timers

You can configure the delay time between when OSPFv2 receives a topology change and when it starts an SPF calculation. You also can configure the hold time between two consecutive SPF calculations.

Procedure

Step 1  Create an OSPFv2 routing process:
router ospf process_id

Example:
ciscoasa(config)# router ospf 2

The process_id argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

Step 2  Configure the route calculation times:
timers throttle spf spf-start spf-hold spf-maximum

Example:
ciscoasa(config-router)# timers throttle spf 500 500 600
The \textit{spf-start} argument is the delay time (in milliseconds) between when OSPF receives a topology change and when it starts an SPF calculation. It can be an integer from 0 to 600000.

The \textit{spf-hold} argument is the minimum time (in milliseconds) between two consecutive SPF calculations. It can be an integer from 0 to 600000.

The \textit{spf-maximum} argument is the maximum time (in milliseconds) between two consecutive SPF calculations. It can be integer from 0 to 600000.

### Log Neighbors Going Up or Down

By default, a syslog message is generated when an OSPFv2 neighbor goes up or down.

Configure the \texttt{log-adj-changes} command if you want to know about OSPFv2 neighbors going up or down without turning on the \texttt{debug ospf adjacency} command. The \texttt{log-adj-changes} command provides a higher level view of the peer relationship with less output. Configure the \texttt{log-adj-changes detail} command if you want to see messages for each state change.

**Procedure**

**Step 1** Create an OSPFv2 routing process:

\begin{verbatim}
router ospf process_id
\end{verbatim}

Example:

```
ciscoasa(config)# router ospf 2
```

The \texttt{process_id} argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

**Step 2** Configure logging for neighbors going up or down:

\begin{verbatim}
log-adj-changes [detail]
\end{verbatim}

### Configure OSPFv3

This section describes how to configure OSPFv3 routing processes.

- Enable OSPFv3, page 23-19
- Configure OSPFv3 Interface Parameters, page 23-20
- Configure OSPFv3 Router Parameters, page 23-25
- Configure OSPFv3 Area Parameters, page 23-27
- Configure OSPFv3 Passive Interfaces, page 23-29
- Configure OSPFv3 Administrative Distance, page 23-29
Enable OSPFv3

To enable OSPFv3, you need to create an OSPFv3 routing process, create an area for OSPFv3, enable an interface for OSPFv3, then redistribute the route into the targeted OSPFv3 routing processes.

Procedure

Step 1 Create an OSPFv3 routing process:
   `ipv6 router ospf process-id`
   Example:
   `ciscoasa(config)# ipv6 router ospf 10`
   The `process-id` argument is an internally used tag for this routing process and can be any positive integer. This tag does not have to match the tag on any other device; it is for internal use only. You can use a maximum of two processes.

Step 2 Enable an interface:
   `interface interface_name`
   Example:
   `ciscoasa(config)# interface Gigabitethernet0/0`

Step 3 Create the OSPFv3 routing process with the specified process ID and an area for OSPFv3 with the specified area ID:
   `ipv6 ospf process-id area area_id`
   Example:
   `ciscoasa(config)# ipv6 ospf 200 area 100`
Configure OSPFv3 Interface Parameters

You can change certain interface-specific OSPFv3 parameters, if necessary. You are not required to change any of these parameters, but the following interface parameters must be consistent across all routers in an attached network: **ipv6 ospf hello-interval** and **ipv6 ospf dead-interval**. If you configure any of these parameters, be sure that the configurations for all routers on your network have compatible values.

**Procedure**

**Step 1** Enable an OSPFv3 routing process:

```
ipv6 router ospf process-id
```

Example:
```
ciscoasa(config-if)# ipv6 router ospf 10
```

The **process-id** argument is an internally used tag for this routing process and can be any positive integer. This tag does not have to match the tag on any other device; it is for internal use only. You can use a maximum of two processes.

**Step 2** Create an OSPFv3 area:

```
ipv6 ospf area [area-num] [instance]
```

Example:
```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
  ospf priority 255
  ipv6 ospf cost 100
  ipv6 ospf 100 area 10 instance 200
```

The **area-num** argument is the area for which authentication is to be enabled and can be either a decimal value or an IP address. The **instance** keyword specifies the area instance ID that is to be assigned to an interface. An interface can have only one OSPFv3 area. You can use the same area on multiple interfaces, and each interface can use a different area instance ID.

**Step 3** Specify the cost of sending a packet on an interface:

```
ipv6 ospf cost interface-cost
```

Example:
```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
```
Step 4  Filter outgoing LSAs to an OSPFv3 interface:

```
ipv6 ospf database-filter all out
```

Example:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
  ospf priority 255
  ipv6 ospf cost 100
  ipv6 ospf 100 area 10 instance 200
  ipv6 ospf database-filter all out
```

All outgoing LSAs are flooded to the interface by default.

Step 5  Set the time period in seconds for which hello packets must not be seen before neighbors indicate that the router is down:

```
ipv6 ospf dead-interval seconds
```

Example:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
  ospf priority 255
  ipv6 ospf cost 100
  ipv6 ospf 100 area 10 instance 200
  ipv6 ospf dead-interval 60
```

The value must be the same for all nodes on the network and can range from 1 to 65535. The default is four times the interval set by the `ipv6 ospf hello-interval` command.

Step 6  Specify the encryption type for an interface:

```
ipv6 ospf encryption {ipsec spi spi esp encryption-algorithm [[key-encryption-type] key] authentication-algorithm [[key-encryption-type] key | null)
```

Example:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
```
Configure OSPFv3

```plaintext
ospf priority 255
ipv6 ospf cost 100
ipv6 ospf 100 area 10 instance 200
ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D
```

The `ipsec` keyword specifies the IP security protocol. The `spi` keyword-argument pair specifies the security policy index, which must be in the range of 256 to 4294967295 and entered as a decimal.

The `esp` keyword specifies the encapsulating security payload. The `encryption-algorithm` argument specifies the encryption algorithm to be used with ESP. Valid values include the following:

- `aes-cdc`—Enables AES-CDC encryption.
- `3des`—Enables 3DES encryption.
- `des`—Enables DES encryption.
- `null`—Specifies ESP with no encryption.

The `key-encryption-type` argument can be one of the following two values:

- `0`—The key is not encrypted.
- `7`—The key is encrypted.

The `key` argument specifies the number used in the calculation of the message digest. The number is 32 hexadecimal digits (16 bytes) long. The size of the key depends on the encryption algorithm used. Some algorithms, such as AES-CDC, allow you to choose the size of the key. The `authentication-algorithm` argument specifies the encryption authentication algorithm to be used, which can be one of the following:

- `md5`—Enables message digest 5 (MD5).
- `sha1`—Enables SHA-1.

The `null` keyword overrides area encryption.

If OSPFv3 encryption is enabled on an interface and a neighbor is on different area (for example, area 0), and you want the ASA to form adjacencies with that area, you must change the area on the ASA. After you have changed the area on the ASA to 0, there is a delay of two minutes before the OSPFv3 adjacency comes up.

**Step 7** Specify the flood reduction of LSAs to the interface:
```
ipv6 ospf flood-reduction
```

Example:
```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
vlan 200
nameif outside
security-level 100
ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
ipv6 address 3001::1/64 standby 3001::8
ipv6 address 6001::1/64 standby 6001::8
ipv6 enable
ospf priority 255
ipv6 ospf cost 100
ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

**Step 8** Specify the interval in seconds between hello packets sent on the interface:
```
ipv6 ospf hello-interval seconds
```

Example:
Configure OSPFv3

ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
  ospf priority 255
  ipv6 ospf cost 100
  ipv6 ospf 100 area 10 instance 200
  ipv6 ospf hello-interval 15

The value must be the same for all nodes on a specific network and can range from 1 to 65535. The default interval is 10 seconds for Ethernet interfaces and 30 seconds for non-broadcast interfaces.

Step 9  Disable the OSPF MTU mismatch detection when DBD packets are received:

  ipv6 ospf mtu-ignore

Example:

ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
  ospf priority 255
  ipv6 ospf cost 100
  ipv6 ospf 100 area 10 instance 200
  ipv6 ospf mtu-ignore

OSPF MTU mismatch detection is enabled by default.

Step 10  Set the OSPF network type to a type other than the default, which depends on the network type:

  ipv6 ospf network {broadcast | point-to-point non-broadcast}

Example:

ciscoasa(config-if)# interface GigabitEthernet3/2.200
  vlan 200
  nameif outside
  security-level 100
  ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
  ipv6 address 3001::1/64 standby 3001::8
  ipv6 address 6001::1/64 standby 6001::8
  ipv6 enable
  ospf priority 255
  ipv6 ospf cost 100
  ipv6 ospf 100 area 10 instance 200
  ipv6 ospf network point-to-point non-broadcast

The point-to-point non-broadcast keyword sets the network type to point-to-point non-broadcast. The broadcast keyword sets the network type to broadcast.

Step 11  Set the router priority, which helps determine the designated router for a network:

  ipv6 ospf priority number-value

Example:

ciscoasa(config-if)# interface GigabitEthernet3/2.200
Configure OSPFv3

Step 12 Configure OSPFv3 router interconnections to non-broadcast networks:

```
ipv6 ospf neighbor ipv6-address [priority number] [poll-interval seconds] [cost number] [database-filter all out]
```

Example:
```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
vlan 200
nameif outside
security-level 100
ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
ipv6 address 3001::1/64 standby 3001::8
ipv6 address 6001::1/64 standby 6001::8
ipv6 enable
ospf priority 255
ipv6 ospf cost 100
ipv6 ospf 100 area 10 instance 200
ipv6 ospf priority 4
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Step 13 Specify the time in seconds between LSA retransmissions for adjacencies that belong to the interface:

```
ipv6 ospf retransmit-interval seconds
```

Example:
```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
vlan 200
nameif outside
security-level 100
ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
ipv6 address 3001::1/64 standby 3001::8
ipv6 address 6001::1/64 standby 6001::8
ipv6 enable
ospf priority 255
ipv6 ospf cost 100
ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-interval 8
```

The time must be greater than the expected round-trip delay between any two routers on the attached network. Valid values range from 1 to 65535 seconds. The default is 5 seconds.

Step 14 Set the estimated time in seconds to send a link-state update packet on the interface:

```
ipv6 ospf transmit-delay seconds
```

Example:
```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
vlan 200
nameif outside
security-level 100
```
Configure OSPFv3

Procedure

Step 1  Enable an OSPFv3 routing process:

```
ipv6 router ospf process-id
```

Example:

```
ciscoasa(config)# ipv6 router ospf 10
```

The `process-id` argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

Step 2  Configure OSPFv3 area parameters:

```
area
```

Example:

```
ciscoasa(config-rtr)# area 10
```

Supported parameters include the area ID as a decimal value from 0 to 4294967295 and the area ID in the IP address format of `A.B.C.D`.

Step 3  Set a command to its default value:

```
default
```

Example:

```
ciscoasa(config-rtr)# default originate
```

The `origin` parameter distributes the default route.

Step 4  Control distribution of default information:

```
default-information
```

Step 5  Define the OSPFv3 route administrative distance based on the route type:

```
distance
```

Example:

```
ciscoasa(config-rtr)# distance 200
```
Supported parameters include the administrative distance with values from 1 to 254 and `ospf` for the OSPFv3 distance.

**Step 6** Suppress the sending of syslog messages with the `lsa` parameter when the router receives a link-state advertisement (LSA) for Type 6 Multicast OSPF (MOSPF) packets:

```
ignore
```

Example:
```
ciscoasa(config-rtr)# ignore lsa
```

**Step 7** Configure the router to send a syslog message when an OSPFv3 neighbor goes up or down:

```
log-adjacency-changes
```

Example:
```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

With the `detail` parameter, all state changes are logged.

**Step 8** Suppress the sending and receiving of routing updates on an interface:

```
passive-interface [interface_name]
```

Example:
```
ciscoasa(config-rtr)# passive-interface inside
```

The `interface_name` argument specifies the name of the interface on which the OSPFv3 process is running.

**Step 9** Configure the redistribution of routes from one routing domain into another according to the following parameters:

- `connected`—Specifies connected routes.
- `ospf`—Specifies OSPFv3 routes.
- `static`—Specifies static routes.

```
redistribute
```

Example:
```
ciscoasa(config-rtr)# redistribute ospf
```

**Step 10** Create a fixed router ID for a specified process with the following parameters:

- `A.B.C.D`—Specifies the OSPF router ID in IP address format.
- `cluster-pool`—Configures an IP address pool when Individual Interface clustering is configured. For more information about IP address pools used in clustering, see Configure an IP Address Pool for Clustering (OSPFv2 and OSPFv3), page 23-16.
- `router-id`

Example:
```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

**Step 11** Configure IPv6 address summaries with valid values from 0 to 128:

```
summary-prefix
```

Example:
Configure OSPFv3

Step 12
Adjust routing timers:
The routing timer parameters are the following:

- **lsa**—Specifies OSPFv3 LSA timers.
- **pacing**—Specifies OSPFv3 pacing timers.
- **throttle**—Specifies OSPFv3 throttle timers.

```
ciscoasa(config)# ipv6 router ospf 10
```
```
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

Configure OSPFv3 Area Parameters

Procedure

Step 1
Enable an OSPFv3 routing process:
```
ipv6 router ospf process-id
```

```
ciscoasa(config)# ipv6 router ospf 1
```

The `process-id` argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535.

This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

Step 2
Set the summary default cost of an NSSA area or a stub area:
```
area area-id default-cost cost
```

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

Step 3
Summarize routes that match the address and mask for border routers only:
```
area area-id range ipv6-prefix/ prefix-length [advertise | not advertise] [cost cost]
```

```
ciscoasa(config-rtr)# area 1 range FE01:1::1/64
```

- The `area-id` argument identifies the area for which routes are to be summarized. The value can be specified as a decimal or an IPv6 prefix.
The IPv6 prefix argument specifies the IPv6 prefix. The prefix-length argument specifies the prefix length.

The advertise keyword sets the address range status to advertised and generates a Type 3 summary LSA.

The not-advertise keyword sets the address range status to DoNotAdvertise.

The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

The cost keyword-argument pair specifies the metric or cost for the summary route, which is used during OSPF SPF calculations to determine the shortest paths to the destination.

Valid values range from 0 to 16777215.

Step 4 Specify an NSSA area:

area area-id nssa

Example:

ciscoasa(config-rtr)# area 1 nssa

Step 5 Specify a stub area:

area area-id stub

Example:

ciscoasa(config-rtr)# area 1 stub

Step 6 Define a virtual link and its parameters:

area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [ttl-security hops hop-count]

Example:

ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5

- The area-id argument identifies the area for which routes are to be summarized. The virtual link keyword specifies the creation of a virtual link neighbor.
- The router-id argument specifies the router ID that is associated with the virtual link neighbor.
- Enter the show ospf or show ipv6 ospf command to display the router ID. There is no default value.
- The hello-interval keyword specifies the time in seconds between the hello packets that are sent on an interface. The hello interval is an unsigned integer that is to be advertised in the hello packets. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192. The default is 10.
- The retransmit-interval seconds keyword-argument pair specifies the time in seconds between LSA retransmissions for adjacencies that belong to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay, and can range from 1 to 8192. The default is 5.
- The transmit-delay seconds keyword-argument pair specifies the estimated time in seconds that is required to send a link-state update packet on the interface. The integer value must be greater than zero. LSAs in the update packet have their own ages incremented by this amount before transmission. The range of values can be from 1 to 8192. The default is 1.
• The **dead-interval seconds** keyword-argument pair specifies the time in seconds that hello packets are not seen before a neighbor indicates that the router is down. The dead interval is an unsigned integer. The default is four times the hello interval, or 40 seconds. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 to 8192.

• The **ttl-security hops** keyword configures the time-to-live (TTL) security on a virtual link. The **hop-count** argument value can range from 1 to 254.

---

### Configure OSPFv3 Passive Interfaces

**Procedure**

**Step 1**
Enable an OSPFv3 routing process:

`ipv6 router ospf process_id`

Example:

```plaintext
ciscoasa(config-if)# ipv6 router ospf 1
```

The **process_id** argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

**Step 2**
Suppress the sending and receiving of routing updates on an interface:

`passive-interface [interface_name]`

Example:

```plaintext
ciscoasa(config-rtr)# passive-interface inside
```

The **interface_name** argument specifies the name of the interface on which the OSPFv3 process is running. If the **no interface_name** argument is specified, all of the interfaces in the OSPFv3 process **process_id** are made passive.

---

### Configure OSPFv3 Administrative Distance

**Procedure**

**Step 1**
Enable an OSPFv3 routing process:

`ipv6 router ospf process_id`

Example:

```plaintext
ciscoasa(config-if)# ipv6 router ospf 1
```
Configure OSPFv3

The `process_id` argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

**Step 2**

Set the administrative distance for OSPFv3 routes:

```
distance [ospf {external | inter-area | intra-area}] distance
```

Example:

```
ciscoasa(config-rtr)# distance ospf external 200
```

The `ospf` keyword specifies OSPFv3 routes. The `external` keyword specifies the external Type 5 and Type 7 routes for OSPFv3. The `inter-area` keyword specifies the inter-area routes for OSPFv3. The `intra-area` keyword specifies the intra-area routes for OSPFv3. The `distance` argument specifies the administrative distance, which is an integer from 10 to 254.

---

**Configure OSPFv3 Timers**

You can set LSA arrival, LSA pacing, and throttling timers for OSPFv3.

**Procedure**

**Step 1**

Enable an OSPFv3 routing process:

```
ipv6 router ospf process-id
```

Example:

```
ciscoasa(config-if)# ipv6 router ospf 1
```

The `process-id` argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

**Step 2**

Set the minimum interval at which the ASA accepts the same LSA from OSPF neighbors:

```
timers lsa arrival milliseconds
```

Example:

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

The `milliseconds` argument specifies the minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 6,000,000 milliseconds. The default is 1000 milliseconds.

**Step 3**

Configure LSA flood packet pacing:

```
timers pacing flood milliseconds
```

Example:

```
ciscoasa(config-rtr)# timers lsa flood 20
```
The `milliseconds` argument specifies the time in milliseconds at which LSAs in the flooding queue are paced in between updates. The configurable range is from 5 to 100 milliseconds. The default value is 33 milliseconds.

**Step 4** Change the interval at which OSPFv3 LSAs are collected into a group and refreshed, checksummed, or aged:

```text
timers pacing lsa-group seconds
```

Example:

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

The `seconds` argument specifies the number of seconds in the interval at which LSAs are grouped, refreshed, checksummed, or aged. The range is from 10 to 1800 seconds. The default value is 240 seconds.

**Step 5** Configure LSA retransmission packet pacing:

```text
timers pacing retransmission milliseconds
```

Example:

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

The `milliseconds` argument specifies the time in milliseconds at which LSAs in the retransmission queue are paced. The configurable range is from 5 to 200 milliseconds. The default value is 66 milliseconds.

**Step 6** Configure OSPFv3 LSA throttling:

```text
timers throttle lsa milliseconds1 milliseconds2 milliseconds3
```

Example:

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- The `milliseconds1` argument specifies the delay in milliseconds to generate the first occurrence of the LSA. The `milliseconds2` argument specifies the maximum delay in milliseconds to originate the same LSA. The `milliseconds3` argument specifies the minimum delay in milliseconds to originate the same LSA.

- For LSA throttling, if the minimum or maximum time is less than the first occurrence value, then OSPFv3 automatically corrects to the first occurrence value. Similarly, if the maximum delay specified is less than the minimum delay, then OSPFv3 automatically corrects to the minimum delay value.

- For `milliseconds1`, the default value is 0 milliseconds.

- For `milliseconds2` and `milliseconds3`, the default value is 5000 milliseconds.

**Step 7** Configure OSPFv3 SPF throttling:

```text
timers throttle spf milliseconds1 milliseconds2 milliseconds3
```

Example:

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- The `milliseconds1` argument specifies the delay in milliseconds to receive a change to the SPF calculation. The `milliseconds2` argument specifies the delay in milliseconds between the first and second SPF calculations. The `milliseconds3` argument specifies the maximum wait time in milliseconds for SPF calculations.

- For SPF throttling, if `milliseconds2` or `milliseconds3` is less than `milliseconds1`, then OSPFv3 automatically corrects to the `milliseconds1` value. Similarly, if `milliseconds3` is less than `milliseconds2`, then OSPFv3 automatically corrects to the `milliseconds2` value.
Configure OSPFv3

For milliseconds1, the default value of SPF throttling is 5000 milliseconds.

For milliseconds2 and milliseconds3, the default value of SPF throttling is 10000 milliseconds.

Define Static OSPFv3 Neighbors

You need to define static OSPFv3 neighbors to advertise OSPF routes over a point-to-point, non-broadcast network. This feature lets you broadcast OSPFv3 advertisements across an existing VPN connection without having to encapsulate the advertisements in a GRE tunnel.

Before you begin, you must create a static route to the OSPFv3 neighbor. See Chapter 20, “Static and Default Routes,” for more information about creating static routes.

Procedure

Step 1 Enable an OSPFv3 routing process and enters IPv6 router configuration mode.

```
ipv6 router ospf process-id
```

Example:

```
ciscoasa(config)# ipv6 router ospf 1
```

The `process-id` argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

Step 2 Configure OSPFv3 router interconnections to non-broadcast networks.

```
ipv6 ospf neighbor ipv6-address [priority number] [poll-interval seconds] [cost number] [database-filter all out]
```

Example:

```
ciscoasa(config-if)# interface ethernet0/0 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Reset OSPFv3 Default Parameters

To return an OSPFv3 parameter to its default value, perform the following steps:

Procedure

Step 1 Enable an OSPFv3 routing process:

```
ipv6 router ospf process-id
```

Example:

```
ciscoasa(config-if)# ipv6 router ospf 1
```
The \textit{process\_id} argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

\textbf{Step 2} \hspace{1em} Return an optional parameter to its default value:

\begin{verbatim}
default [area | auto-cost | default-information | default-metric | discard-route |
discard-route | distance | distribute-list | ignore | log-adjacency-changes |
maximum-paths | passive-interface | redistribute | router-id | summary-prefix | timers]
\end{verbatim}

Example:

\begin{verbatim}
ciscoasa(config-rtr)# default metric 5
\end{verbatim}

- The \textit{area} keyword specifies the OSPFv3 area parameters. The \textit{auto-cost} keyword specifies the OSPFv3 interface cost according to bandwidth.
- The \textit{default-information} keyword distributes default information. The \textit{default-metric} keyword specifies the metric for a redistributed route.
- The \textit{discard-route} keyword enables or disables the discard-route installation. The \textit{distance} keyword specifies the administrative distance.
- The \textit{distribute-list} keyword filters networks in routing updates.
- The \textit{ignore} keyword ignores a specific event. The \textit{log-adjacency-changes} keyword logs changes in the adjacency state.
- The \textit{maximum-paths} keyword forwards packets over multiple paths.
- The \textit{passive-interface} keyword suppresses routing updates on an interface.
- The \textit{redistribute} keyword redistributes IPv6 prefixes from another routing protocol.
- The \textit{router-id} keyword specifies the router ID for the specified routing process.
- The \textit{summary-prefix} keyword specifies the IPv6 summary prefix.
- The \textit{timers} keyword specifies the OSPFv3 timers.

\section*{Send Syslog Messages}

Configure the router to send a syslog message when an OSPFv3 neighbor goes up or down.

\textbf{Procedure}

\begin{enumerate}
\item \textbf{Step 1} \hspace{1em} Enable an OSPFv3 routing process:
\begin{verbatim}
ipv6 router ospf process-id
\end{verbatim}

Example:

\begin{verbatim}
ciscoasa(config-if)# ipv6 router ospf 1
\end{verbatim}

The \textit{process-id} argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

\item \textbf{Step 2} \hspace{1em} Configure the router to send a syslog message when an OSPFv3 neighbor goes up or down:
log-adjacency-changes [detail]

Example:
ciscoasa(config-rtr)# log-adjacency-changes detail

The detail keyword sends a syslog message for each state, not only when an OSPFv3 neighbor goes up or down.

**Suppress Syslog Messages**

To suppress the sending of syslog messages when the route receives unsupported LSA Type 6 multicast OSPF (MOSPF) packets, perform the following steps:

**Procedure**

**Step 1** Enable an OSPFv2 routing process:

```
router ospf process_id
```

Example:
ciscoasa(config-if)# router ospf 1

The process_id argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

**Step 2** Suppress the sending of syslog messages when the router receives unsupported LSA Type 6 MOSPF packets:

```
ignore lsa mospf
```

Example:
ciscoasa(config-rtr)# ignore lsa mospf

**Calculate Summary Route Costs**

**Procedure**

**Step 1** Restore the methods that are used to calculate summary route costs according to RFC 1583:

```
compatible rfc1583
```

Example:
ciscoasa (config-rtr)# compatible rfc1583
Generate a Default External Route into an OSPFv3 Routing Domain

Procedure

Step 1  Enable an OSPFv3 routing process:

```
ipv6 router ospf process-id
```

Example:
```
ciscoasa(config-if)# ipv6 router ospf 1
```

The `process-id` argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

Step 2  Generate a default external route into an OSPFv3 routing domain:

```
default-information originate [always] metric metric-value [metric-type type-value] [route-map map-name]
```

Example:
```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
```

- The `always` keyword advertises the default route whether or not the default route exists.
- The `metric metric-value` keyword-argument pair specifies the metric used for generating the default route.
- If you do not specify a value using the `default-metric` command, the default value is 10. Valid metric values range from 0 to 16777214.
- The `metric-type type-value` keyword-argument pair specifies the external link type that is associated with the default route that is advertised into the OSPFv3 routing domain. Valid values can be one of the following:
  - 1—Type 1 external route
  - 2—Type 2 external route

The default is the type 2 external route.

- The `route-map map-name` keyword-argument pair specifies the routing process that generates the default route if the route map is satisfied.

Configure an IPv6 Summary Prefix

Procedure

Step 1  Enable an OSPFv3 routing process:

```
ipv6 router ospf
process-id
```

Configure OSPFv3

Example:
ciscoasa(config-if)# ipv6 router ospf 1

The process_id argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

**Step 2** Configure an IPv6 summary prefix:

```
summary-prefix prefix [not-advertise | tag tag-value]
```

Example:
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# router-id 192.168.3.3
ciscoasa(config-rtr)# summary-prefix FECO::/24
ciscoasa(config-rtr)# redistribute static

The prefix argument is the IPv6 route prefix for the destination. The not-advertise keyword suppresses routes that match the specified prefix and mask pair. This keyword applies to OSPFv3 only. The tag tag-value keyword-argument pair specifies the tag value that can be used as a match value for controlling redistribution through route maps. This keyword applies to OSPFv3 only.

---

**Redistribute IPv6 Routes**

Procedure

**Step 1** Enable an OSPFv3 routing process:

```
ipv6 router ospf process-id
```

Example:
ciscoasa(config-if)# ipv6 router ospf 1

The process-id argument is an internally used identifier for this routing process, is locally assigned, and can be any positive integer from 1 to 65535. This ID does not have to match the ID on any other device; it is for internal administrative use only. You can use a maximum of two processes.

**Step 2** Redistribute IPv6 routes from one OSPFv3 process into another:

```
redistribute source-protocol [process-id] [include-connected {level-1 | level-2}] [as-number] [metric metric-value | transparent] [metric-type type-value] [match {external [1|2] | internal | nssa-external [1|2]}] [tag tag-value] [route-map map-tag]
```

Example:
ciscoasa(config-rtr)# redistribute connected 5 type-1

- The source-protocol argument specifies the source protocol from which routes are being redistributed, which can be static, connected, or OSPFv3.
- The process-id argument is the number that is assigned administratively when the OSPFv3 routing process is enabled.
• The **include-connected** keyword allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.

• The **level-1** keyword specifies that for Intermediate System-to-Intermediate System (IS-IS), Level 1 routes are redistributed into other IP routing protocols independently.

• The **level-1-2** keyword specifies that for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.

• The **level-2** keyword specifies that for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.

• For the **metric** metric-value keyword-argument pair, when redistributing routes from one OSPFv3 process into another OSPFv3 process on the same router, the metric is carried through from one process to the other if no metric value is specified. When redistributing other processes into an OSPFv3 process, the default metric is 20 when no metric value is specified.

• The **metric transparent** keyword causes RIP to use the routing table metric for redistributed routes as the RIP metric.

• The **metric-type** type-value keyword-argument pair specifies the external link type that is associated with the default route that is advertised into the OSPFv3 routing domain. Valid values can be one of the following: 1 for a Type 1 external route or 2 for a Type 2 external route. If no value is specified for the **metric-type** keyword, the ASA adopts a Type 2 external route. For IS-IS, the link type can be one of the following: internal for an IS-IS metric that is less than 63 or external for an IS-IS metric that is greater than 64 and less than 128. The default is internal.

• The **match** keyword redistributes routes into other routing domains and is used with one of the following options: external [1|2] for routes that are external to the autonomous system, but are imported into OSPFv3 as Type 1 or Type 2 external routes; internal for routes that are internal to a specific autonomous system; nssa-external [1|2] for routes that are external to the autonomous system, but are imported into OSPFv3 in an NSSA for IPv6 as Type 1 or Type 2 external routes.

• The **tag** tag-value keyword-argument pair specifies the 32-bit decimal value that is attached to each external route, which may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP. For other protocols, zero is used. Valid values range from 0 to 4294967295.

• The **route-map** keyword specifies the route map to check for filtering the importing of routes from the source routing protocol to the current routing protocol. If this keyword is not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes are imported. The **map-tag** argument identifies a configured route map.

---

**Configure Graceful Restart**

The ASA may experience some known failure situations, that should not affect packet forwarding across the switching platform. The Non-Stop Forwarding (NSF) capability allows data forwarding to continue along known routes, while the routing protocol information is being restored. This capability is useful when there is a component failure (i.e., active unit crash with standby unit taking over in failover (HA) mode, master unit crash with slave unit elected as new master in cluster mode), or when there is a scheduled hitless software upgrade.
Graceful restart is supported on both OSPFv2 and OSPFv3. You can configure graceful restart on OSPFv2 by using either using NSF Cisco (RFC 4811 and RFC 4812) or NSF IETF (RFC 3623). You can configure graceful restart on OSPFv3 using graceful-restart (RFC 5187).

Configuring the NSF graceful-restart feature involves two steps; configuring capabilities and configuring a device as NSF-capable or NSF-aware. A NSF-capable device can indicate its own restart activities to neighbors and a NSF-aware device can help a restarting neighbor.

A device can be configured as NSF-capable or NSF-aware, depending on some conditions:

- A device can be configured as NSF-aware irrespective of the mode in which it is.
- A device has to be in either Failover or Spanned Etherchannel (L2) cluster mode to be configured as NSF-capable.
- For a device to be either NSF-aware or NSF-capable, it should be configured with the capability of handling opaque Link State Advertisements (LSAs)/ Link Local Signaling (LLS) block as required.

---

**Note**

When fast hellos are configured for OSPFv2, graceful restart does not occur when the active unit reloads and the standby unit becomes active. This is because the time taken for the role change is more than the configured dead interval.

### Configure capabilities

The Cisco NSF Graceful Restart mechanism depends on the LLS capability as it sends an LLS block with the RS-bit set in the Hello packet, to indicate the restart activity. The IETF NSF mechanism depends on the opaque LSA capability as it sends opaque-LSAs of type-9 to indicate the restart activity. To configure capabilities enter the following commands:

**Procedure**

**Step 1** Create an OSPF routing process and enters router configuration mode for the OSPF process that you want to redistribute:

```
router ospf process_id
```

Example:

```
ciscoasa(config)# router ospf 2
```

The `process_id` argument is an internally used identifier for this routing process and can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

**Step 2** Enable the use of LLS data block or opaque LSAs to enable NSF:

```
capability {lls|opaque}
```

Example:

```
ciscoasa(config-router)# capability lls
```

The `lls` keyword is used to enable LLS capability for Cisco NSF Graceful Restart mechanism. The `opaque` keyword is used to enable opaque LSA capability for IETF NSF Graceful Restart mechanism.
Configuring Graceful Restart for OSPFv2

There are two graceful restart mechanisms for OSPFv2, Cisco NSF and IETF NSF. Only one of these graceful restart mechanisms can be configured at a time for an ospf instance. An NSF-aware device can be configured as both Cisco NSF helper and IETF NSF helper but a NSF-capable device can be configured in either Cisco NSF or IETF NSF mode at a time for an ospf instance.

Configure Cisco NSF Graceful Restart for OSPFv2

Configure Cisco NSF Graceful Restart for OSPFv2, for a NSF-capable or NSF-aware device.

Procedure

---

**Step 1**
Enable Cisco NSF on a NSF-capable device:

```
nsf cisco [enforce global]
```

Example:

```
ciscoasa(config-router)# nsf cisco
```

The `enforce global` keyword cancels NSF restart when non-NSF-aware neighbor devices are detected.

**Step 2**
Enable Cisco NSF helper mode on NSF-aware device:

```
capability {lls|opaque}
```

Example:

```
ciscoasa(config-router)# capability lls
```

This command is enabled by default. Using the no form of the command disables it.

---

Configure IETF NSF Graceful Restart for OSPFv2

Configure IETF NSF Graceful Restart for OSPFv2, for a NSF-capable or NSF-aware device.

Procedure

---

**Step 1**
Enable IETF NSF on a NSF-capable device:

```
nsf ietf [restart interval seconds]
```

Example:

```
ciscoasa(config-router)# nsf ietf restart interval 80
```

The `restart interval seconds` specifies the length of the graceful restart interval, in seconds. Valid values are from 1 to 1800 seconds. The default value is 120 seconds.
Step 2 Enable IETF NSF helper mode on NSF-aware device:

```
nsf ietf helper [strict-lsa-checking]
```

Example:
```
ciscoasa(config-router)# nsf ietf helper
```

The `strict-LSA-checking` keyword indicates that the helper router will terminate the process of the restarting router if it detects that there is a change to a LSA that would be flooded to the restarting router, or if there is a changed LSA on the retransmission list of the restarting router when the graceful restart process is initiated.

This command is enabled by default. Using the no form of the command disables it.

---

**Configuring Graceful Restart for OSPFv3**

Configuring the NSF graceful-restart feature for OSPFv3 involves two steps; configuring a device to be NSF-capable and then configuring a device to be NSF-aware.

**Procedure**

Step 1 Enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address:

```
interface physical_interface
ipv6 enable
```

Example:
```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

The `physical_interface` argument identifies the interface that participates in OSPFv3 NSF.

Step 2 Enable graceful-restart for OSPFv3 on a NSF-capable device:

```
graceful-restart [restart interval seconds]
```

Example:
```
ciscoasa(config-router)# graceful-restart restart interval 80
```

The `restart interval seconds` specifies the length of the graceful restart interval, in seconds. Valid values are from 1 to 1800 seconds. The default value is 120 seconds.

Graceful restart might be terminated when restart interval is configured with a value less than the time taken for the adjacency to come up. For example, a restart interval below 30 seconds, is not supported.

Step 3 Enable graceful-restart for OSPFv3 on a NSF-aware device:

```
graceful-restart helper [strict-lsa-checking]
```

Example:
```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

Graceful restart might be terminated when restart interval is configured with a value less than the time taken for the adjacency to come up. For example, a restart interval below 30 seconds, is not supported.
The **strict-LSA-checking** keyword indicates that the helper router will terminate the process of the restarting router if it detects that there is a change to a LSA that would be flooded to the restarting router, or if there is a changed LSA on the retransmission list of the restarting router when the graceful restart process is initiated.

The graceful-restart helper mode is enabled by default.

---

**Remove the OSPF Configuration**

Remove the OSPFv2 configuration.

**Procedure**

**Step 1** Remove the entire OSPFv2 configuration that you have enabled.

`clear configure router ospf pid`

Example:

```
ciscoasa(config)# clear configure router ospf 1000
```

After the configuration is cleared, you must reconfigure OSPF using the `router ospf` command.

Remove the OSPFv3 configuration.

**Procedure**

**Step 1** Remove the entire OSPFv3 configuration that you have enabled:

`clear configure ipv6 router ospf process-id`

Example:

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

After the configuration is cleared, you must reconfigure OSPFv3 using the `ipv6 router ospf` command.

---

**Example for OSPFv2**

The following example shows how to enable and configure OSPFv2 with various optional processes:

**Step 1** To enable OSPFv2, enter the following commands:

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```
Example for OSPFv2

Step 2  
(Optional) To redistribute routes from one OSPFv2 process to another OSPFv2 process, enter the following commands:

```bash
ciscoasa(config)# route-map 1-to-2 permit  
ciscoasa(config-route-map)# match metric 1  
ciscoasa(config-route-map)# set metric 5  
ciscoasa(config-route-map)# set metric-type type-1  
ciscoasa(config-route-map)# router ospf 2  
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

Step 3  
(Optional) To configure OSPFv2 interface parameters, enter the following commands:

```bash
ciscoasa(config)# router ospf 2  
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0  
ciscoasa(config-router)# interface inside  
ciscoasa(config-interface)# ospf cost 20  
ciscoasa(config-interface)# ospf retransmit-interval 15  
ciscoasa(config-interface)# ospf transmit-delay 10  
ciscoasa(config-interface)# ospf priority 20  
ciscoasa(config-interface)# ospf hello-interval 10  
ciscoasa(config-interface)# ospf dead-interval 40  
ciscoasa(config-interface)# ospf authentication-key cisco  
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco  
ciscoasa(config-interface)# ospf authentication message-digest
```

Step 4  
(Optional) To configure OSPFv2 area parameters, enter the following commands:

```bash
ciscoasa(config)# router ospf 2  
ciscoasa(config-rtr)# area 0 authentication  
ciscoasa(config-rtr)# area 0 authentication message-digest  
ciscoasa(config-rtr)# area 17 stub  
ciscoasa(config-rtr)# area 17 default-cost 20
```

Step 5  
(Optional) To configure the route calculation timers and show the log neighbor up and down messages, enter the following commands:

```bash
ciscoasa(config-rtr)# timers spf 10 120  
ciscoasa(config-rtr)# log-adj-changes [detail]
```

Step 6  
(Optional) To show current OSPFv2 configuration settings, enter the `show ospf` command.

The following is sample output from the `show ospf` command:

```bash
ciscoasa(config)# show ospf

Routing Process "ospf 2" with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x 0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
  Number of interfaces in this area is 1
  Area has no authentication
  SPF algorithm executed 2 times
  Area ranges are
  Number of LSA 5. Checksum Sum 0x 209a3
  Number of opaque link LSA 0. Checksum Sum 0x 0
  Number of DCbitless LSA 0
  Number of indication LSA 0
```
Step 7 To clear the OSPFv2 configuration, enter the following command:

ciscoasa(config)# clear configure router ospf pid

Examples for OSPFv3

The following example shows how to enable and configure OSPFv3 at the interface level:

ciscoasa (config)# interface GigabitEthernet3/1
  ciscoasa (config-if)# ipv6 enable
  ciscoasa (config-if)# ipv6 ospf 1 area 1

The following is sample output from the `show running-config ipv6` command:

ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
  log-adjacency-changes

The following is sample output from the `show running-config interface` command:

ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
  interface GigabitEthernet3/1
  nameif fda
  security-level 100
  ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
  ipv6 address 9098::10/64 standby 9098::11
  ipv6 enable
  ipv6 ospf 1 area 1

The following examples show how to configure OSPFv3-specific interfaces:

ciscoasa (config)# interface GigabitEthernet3/1
  ciscoasa (config-if)# nameif fda
  ciscoasa (config-if)# security-level 100
  ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
  ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
  ciscoasa (config-if)# ipv6 enable
  ciscoasa (config-if)# ipv6 ospf cost 900
  ciscoasa (config-if)# ipv6 ospf hello-interval 20
  ciscoasa (config-if)# ipv6 ospf network broadcast
  ciscoasa (config-if)# ipv6 ospf database-filter all out
  ciscoasa (config-if)# ipv6 ospf flood-reduction
  ciscoasa (config-if)# ipv6 ospf mtu-ignore
  ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
  ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
  12345678901234567890123456789012
  ciscoasa (config-if)# ipv6 ospf database-filter all out
  ciscoasa (config-if)# ipv6 ospf flood-reduction
  ciscoasa (config-if)# ipv6 ospf mtu-ignore
  ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
  ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
  12345678901234567890123456789012

  ciscoasa (config)# ipv6 router ospf 1
  ciscoasa (config)# area 1 nssa
  ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
  ciscoasa (config)# timers lsa arrival 900
  ciscoasa (config)# timers pacing flood 100
  ciscoasa (config)# timers throttle lsa 900 900 900
  ciscoasa (config)# passive-interface fda
  ciscoasa (config)# log-adjacency-changes
  ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
For an example of how to configure an OSPFv3 virtual link, see the following URL:

Monitoring OSPF

You can display specific statistics such as the contents of IP routing tables, caches, and databases. You can also use the information provided to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path that your device packets are taking through the network.

To monitor or display various OSPFv2 routing statistics, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ospf [process-id [area-id]]</code></td>
<td>Displays general information about OSPFv2 routing processes.</td>
</tr>
<tr>
<td><code>show ospf border-routers</code></td>
<td>Displays the internal OSPFv2 routing table entries to the ABR and ASBR.</td>
</tr>
<tr>
<td><code>show ospf [process-id [area-id]] database</code></td>
<td>Displays lists of information related to the OSPFv2 database for a specific router.</td>
</tr>
<tr>
<td><code>show ospf flood-list if-name</code></td>
<td>Displays a list of LSAs waiting to be flooded over an interface (to observe OSPF v2 packet pacing). OSPFv2 update packets are automatically paced so they are not sent less than 33 milliseconds apart. Without pacing, some update packets could get lost in situations where the link is slow, a neighbor could not receive the updates quickly enough, or the router could run out of buffer space. For example, without pacing, packets might be dropped if either of the following topologies exist:</td>
</tr>
<tr>
<td></td>
<td>• A fast router is connected to a slower router over a point-to-point link.</td>
</tr>
<tr>
<td></td>
<td>• During flooding, several neighbors send updates to a single router at the same time. Pacing is also used between resends to increase efficiency and minimize lost retransmissions. You also can display the LSAs waiting to be sent out of an interface. Pacing enables OSPFv2 update and retransmission packets to be sent more efficiently. There are no configuration tasks for this feature; it occurs automatically.</td>
</tr>
<tr>
<td><code>show ospf interface [if_name]</code></td>
<td>Displays OSPFv2-related interface information.</td>
</tr>
<tr>
<td><code>show ospf neighbor [interface-name] [neighbor-id] [detail]</code></td>
<td>Displays OSPFv2 neighbor information on a per-interface basis.</td>
</tr>
<tr>
<td><code>show ospf request-list neighbor if_name</code></td>
<td>Displays a list of all LSAs requested by a router.</td>
</tr>
</tbody>
</table>
Monitoring OSPF

To monitor or display various OSPFv3 routing statistics, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ospf retransmission-list neighbor if_name</code></td>
<td>Displays a list of all LSAs waiting to be resent.</td>
</tr>
<tr>
<td><code>show ospf [process-id] summary-address</code></td>
<td>Displays a list of all summary address redistribution information configured under an OSPFv2 process.</td>
</tr>
<tr>
<td><code>show ospf [process-id] traffic</code></td>
<td>Displays a list of different types of packets being sent or received by a specific OSPFv2 instance.</td>
</tr>
<tr>
<td><code>show ospf [process-id] virtual-links</code></td>
<td>Displays OSPFv2-related virtual links information.</td>
</tr>
<tr>
<td><code>show route cluster</code></td>
<td>Displays additional OSPFv2 route synchronization information in clustering.</td>
</tr>
</tbody>
</table>

To monitor or display various OSPFv3 routing statistics, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 ospf [process-id [area-id]]</code></td>
<td>Displays general information about OSPFv3 routing processes.</td>
</tr>
<tr>
<td><code>show ipv6 ospf [process-id] border-routers</code></td>
<td>Displays the internal OSPFv3 routing table entries to the ABR and ASBR.</td>
</tr>
<tr>
<td>`show ipv6 ospf [process-id [area-id]] database [external</td>
<td>inter-area prefix</td>
</tr>
<tr>
<td><code>show ipv6 ospf [process-id [area-id]] events</code></td>
<td>Displays OSPFv3 event information.</td>
</tr>
</tbody>
</table>
### Command | Purpose
--- | ---
`show ipv6 ospf [process-id] [area-id] flood-list interface-type interface-number` | Displays a list of LSAs waiting to be flooded over an interface (to observe OSPFv3 packet pacing). OSPFv3 update packets are automatically paced so they are not sent less than 33 milliseconds apart. Without pacing, some update packets could get lost in situations where the link is slow, a neighbor could not receive the updates quickly enough, or the router could run out of buffer space. For example, without pacing, packets might be dropped if either of the following topologies exist:

- A fast router is connected to a slower router over a point-to-point link.
- During flooding, several neighbors send updates to a single router at the same time.

Pacing is also used between retransmissions to increase efficiency and minimize lost retransmissions. You also can display the LSAs waiting to be sent out of an interface. Pacing enables OSPFv3 update and retransmission packets to be sent more efficiently.

There are no configuration tasks for this feature; it occurs automatically.

`show ipv6 ospf [process-id] [area-id] interface [type number] [brief]` | Displays OSPFv3-related interface information.

`show ipv6 ospf neighbor [process-id] [area-id] [interface-type interface-number] [neighbor-id] [detail]` | Displays OSPFv3 neighbor information on a per-interface basis.

`show ipv6 ospf [process-id] [area-id] request-list [neighbor] [interface] [interface-neighbor]` | Displays a list of all LSAs requested by a router.

`show ipv6 ospf [process-id] [area-id] retransmission-list [neighbor] [interface] [interface-neighbor]` | Displays a list of all LSAs waiting to be resent.

`show ipv6 ospf statistic [process-id] [detail]` | Displays various OSPFv3 statistics.

`show ipv6 ospf [process-id] summary-prefix` | Displays a list of all summary address redistribution information configured under an OSPFv3 process.


`show ipv6 ospf virtual-links` | Displays OSPFv3-related virtual links information.

`show ipv6 route cluster [failover] [cluster] [interface] [ospf] [summary]` | Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number in a cluster.
Additional References

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2328</td>
<td>OSPFv2</td>
</tr>
<tr>
<td>4552</td>
<td>OSPFv3 Authentication</td>
</tr>
<tr>
<td>5340</td>
<td>OSPF for IPv6</td>
</tr>
</tbody>
</table>

History for OSPF

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Support</td>
<td>7.0(1)</td>
<td>Support was added for route data, authentication, and redistribution and monitoring of routing information using the Open Shortest Path First (OSPF) routing protocol. We introduced the following command: <code>route ospf</code></td>
</tr>
</tbody>
</table>
### Table 23-1 Feature History for OSPF (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Routing in Multiple Context Mode</td>
<td>9.0(1)</td>
<td>OSPFv2 routing is supported in multiple context mode.</td>
</tr>
<tr>
<td>Clustering</td>
<td></td>
<td>For OSPFv2 and OSPFv3, bulk synchronization, route synchronization, and Spanned EtherChannel load balancing are supported in the clustering environment. We introduced or modified the following commands: <code>show route cluster</code>, <code>show ipv6 route cluster</code>, <code>debug route cluster</code>, <code>router-id cluster-pool</code>.</td>
</tr>
<tr>
<td>OSPFv3 Support for IPv6</td>
<td></td>
<td>OSPFv3 routing is supported for IPv6. We introduced or modified the following commands: <code>ipv6 ospf</code>, <code>ipv6 ospf area</code>, <code>ipv6 ospf cost</code>, <code>ipv6 ospf database-filter all out</code>, <code>ipv6 ospf dead-interval</code>, <code>ipv6 ospf encryption</code>, <code>ipv6 ospf hello-interval</code>, <code>ipv6 ospf mtu-ignore</code>, <code>ipv6 ospf neighbor</code>, <code>ipv6 ospf network</code>, <code>ipv6 ospf flood-reduction</code>, <code>ipv6 ospf priority</code>, <code>ipv6 ospf retransmit-interval</code>, <code>ipv6 ospf transmit-delay</code>, <code>ipv6 router ospf</code>, <code>ipv6 router ospf area</code>, <code>ipv6 router ospf default</code>, <code>ipv6 router ospf default-information</code>, <code>ipv6 router ospf distance</code>, <code>ipv6 router ospf exit</code>, <code>ipv6 router ospf ignore</code>, <code>ipv6 router ospf log-adjacency-changes</code>, <code>ipv6 router ospf no</code>, <code>ipv6 router ospf passive-interface</code>, <code>ipv6 router ospf redistribute</code>, <code>ipv6 router ospf router-id</code>, <code>ipv6 router ospf summary-prefix</code>, <code>ipv6 router ospf timers</code>, <code>area encryption</code>, <code>area range</code>, <code>area stub</code>, <code>area nssa</code>, <code>area virtual-link</code>, <code>default</code>, <code>default-information originate</code>, <code>distance</code>, <code>ignore lsa mospf</code>, <code>log-adjacency-changes</code>, <code>redistribute</code>, <code>router-id</code>, <code>summary-prefix</code>, <code>timers lsa arrival</code>, <code>timers pacing flood</code>, <code>timers pacing lsa-group</code>, <code>timers pacing retransmission</code>, <code>timers throttle</code>, <code>show ipv6 ospf</code>, <code>show ipv6 ospf border-routers</code>, <code>show ipv6 ospf database</code>, <code>show ipv6 ospf events</code>, <code>show ipv6 ospf flood-list</code>, <code>show ipv6 ospf graceful-restart</code>, <code>show ipv6 ospf interface</code>, <code>show ipv6 ospf neighbor</code>, <code>show ipv6 ospf request-list</code>, <code>show ipv6 ospf retransmission-list</code>, <code>show ipv6 ospf statistic</code>, <code>show ipv6 ospf summary-prefix</code>, <code>show ipv6 ospf timers</code>, <code>show ipv6 ospf traffic</code>, <code>show ipv6 ospf virtual-links</code>, <code>show ospf</code>, <code>show running-config ipv6 router</code>, <code>clear ipv6 ospf</code>, <code>clear configure ipv6 router</code>, <code>debug ospfv3</code>, <code>ipv6 ospf neighbor</code>.</td>
</tr>
</tbody>
</table>
OSPF support for Fast Hellos

9.2(1) OSPF supports the Fast Hello Packets feature, resulting in a configuration that results in faster convergence in an OSPF network.

We modified the following command: `ospf dead-interval`

Timers

New OSPF timers were added; old ones were deprecated.

We introduced the following commands: `timers lsa arrival`, `timers pacing`, `timers throttle`

We removed the following commands: `Timers spf`, `timers lsa-grouping-pacing`

Route filtering using access-list

Route filtering using ACL is now supported.

We introduced the following command: `distribute-list`

We introduced the following screen:

OSPF Monitoring enhancements

Additional OSPF monitoring information was added.

We modified the following commands: `show ospf events`, `show ospf rib`, `show ospf statistics`, `show ospf border-routers [detail]`, `show ospf interface brief`

OSPF redistribute BGP

OSPF redistribution feature was added.

We added the following command: `redistribute bgp`

OSPF Support for Non-Stop Forwarding (NSF)

9.3(1) OSPFv2 and OSPFv3 support for NSF was added.

We added the following commands: `capability`, `nssf cisco`, `nssf cisco helper`, `nsf ief`, `nssf ief helper`, `nssf ief helper strict-lsa-checking`, `graceful-restart`, `graceful-restart helper`, `graceful-restart helper strict-lsa-checking`
EIGRP

This chapter describes how to configure the Cisco ASA to route data, perform authentication, and redistribute routing information using the Enhanced Interior Gateway Routing Protocol (EIGRP).

- About EIGRP, page 24-1
- Guidelines for EIGRP, page 24-2
- Configure EIGRP, page 24-3
- Customize EIGRP, page 24-5
- Monitoring for EIGRP, page 24-18
- Example for EIGRP, page 24-18
- History for EIGRP, page 24-19

About EIGRP

EIGRP is an enhanced version of IGRP developed by Cisco. Unlike IGRP and RIP, EIGRP does not send out periodic route updates. EIGRP updates are sent out only when the network topology changes. Key capabilities that distinguish EIGRP from other routing protocols include fast convergence, support for variable-length subnet mask, support for partial updates, and support for multiple network layer protocols.

A router running EIGRP stores all the neighbor routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found. Its support for variable-length subnet masks permits routes to be automatically summarized on a network number boundary. In addition, EIGRP can be configured to summarize on any bit boundary at any interface. EIGRP does not make periodic updates. Instead, it sends partial updates only when the metric for a route changes. Propagation of partial updates is automatically bounded so that only those routers that need the information are updated. As a result of these two capabilities, EIGRP consumes significantly less bandwidth than IGRP.

Neighbor discovery is the process that the ASA uses to dynamically learn of other routers on directly attached networks. EIGRP routers send out multicast hello packets to announce their presence on the network. When the ASA receives a hello packet from a new neighbor, it sends its topology table to the neighbor with an initialization bit set. When the neighbor receives the topology update with the initialization bit set, the neighbor sends its topology table back to the ASA.
The hello packets are sent out as multicast messages. No response is expected to a hello message. The exception to this is for statically defined neighbors. If you use the `neighbor` command, or configure the Hello Interval in ASDM, to configure a neighbor, the hello messages sent to that neighbor are sent as unicast messages. Routing updates and acknowledgements are sent out as unicast messages.

Once this neighbor relationship is established, routing updates are not exchanged unless there is a change in the network topology. The neighbor relationship is maintained through the hello packets. Each hello packet received from a neighbor includes a hold time. This is the time in which the ASA can expect to receive a hello packet from that neighbor. If the ASA does not receive a hello packet from that neighbor within the hold time advertised by that neighbor, the ASA considers that neighbor to be unavailable.

The EIGRP protocol uses four key algorithm technologies, four key technologies, including neighbor discovery/recovery, Reliable Transport Protocol (RTP), and DUAL, which is important for route computations. DUAL saves all routes to a destination in the topology table, not just the least-cost route. The least-cost route is inserted into the routing table. The other routes remain in the topology table. If the main route fails, another route is chosen from the feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination. The feasibility calculation guarantees that the path is not part of a routing loop.

If a feasible successor is not found in the topology table, a route recomputation must occur. During route recomputation, DUAL queries the EIGRP neighbors for a route, who in turn query their neighbors. Routers that do not have a feasible successor for the route return an unreachable message.

During route recomputation, DUAL marks the route as active. By default, the ASA waits for three minutes to receive a response from its neighbors. If the ASA does not receive a response from a neighbor, the route is marked as stuck-in-active. All routes in the topology table that point to the unresponsive neighbor as a feasibility successor are removed.

---

**Note**

EIGRP neighbor relationships are not supported through the IPsec tunnel without a GRE tunnel.

---

**Guidelines for EIGRP**

**Firewall Mode Guidelines**

Supported only in routed firewall mode. Transparent firewall mode is not supported.

**Failover Guidelines**

Supports Stateful Failover in single and multiple context mode.

**IPv6 Guidelines**

Does not support IPv6.

**Clustering Guidelines**

- Supports Spanned EtherChannel and Individual Interface clustering when configured to use both EIGRP and OSPFv2.
- In a Individual Interface cluster setup, EIGRP adjacencies can only be established between two contexts on a shared interface on the master unit. You can manually configure multiple neighbor statements corresponding to each cluster node separately to work around this issue.
Configure EIGRP

This section describes how to enable the EIGRP process on your system. After you have enabled EIGRP, see the following sections to learn how to customize the EIGRP process on your system.

- Enable EIGRP, page 24-3
- Enable EIGRP Stub Routing, page 24-4

Enable EIGRP

You can only enable one EIGRP routing process on the ASA.

To enable EIGRP, perform the following steps:

Procedure

**Step 1** Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
router eigrp as-num
```

Example:

ciscoasa(config)# router eigrp 2

The *as-num* argument is the autonomous system number of the EIGRP routing process.

**Step 2** Configure the interfaces and networks that participate in EIGRP routing:

```
network ip-addr [mask]
```

Example:

ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0

You can configure one or more *network* statements with this command.

Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure Interfaces for EIGRP, page 24-6.
Enable EIGRP Stub Routing

You can enable, and configure the ASA as an EIGRP stub router. Stub routing decreases memory and processing requirements on the ASA. As a stub router, the ASA does not need to maintain a complete EIGRP routing table because it forwards all nonlocal traffic to a distribution router. Generally, the distribution router need not send anything more than a default route to the stub router.

Only specified routes are propagated from the stub router to the distribution router. As a stub router, the ASA responds to all queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message “inaccessible.” When the ASA is configured as a stub, it sends a special peer information packet to all neighboring routers to report its status as a stub router. Any neighbor that receives a packet informing it of the stub status will not query the stub router for any routes, and a router that has a stub peer will not query that peer. The stub router depends on the distribution router to send the correct updates to all peers.

To enable the ASA as an EIGRP stub routing process, perform the following steps:

**Procedure**

**Step 1** Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
router eigrp as-num
```

Example:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

**Step 2** Configure the interfaces and networks that participate in EIGRP routing:

```
network ip-addr [mask]
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

You can configure one or more `network` statements with this command.

Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see section `Configure Passive Interfaces`, page 24-8.

**Step 3** Configure the stub routing process:

```
eigrp stub {receive-only | [connected] [redistributed] [static] [summary]}
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static] [summary]}
```

You must specify which networks are advertised by the stub routing process to the distribution router. Static and connected networks are not automatically redistributed into the stub routing process.
Customize EIGRP

This section describes how to customize the EIGRP routing.

- Define a Network for an EIGRP Routing Process, page 24-5
- Configure Interfaces for EIGRP, page 24-6
- Configure Passive Interfaces, page 24-8
- Configure the Summary Aggregate Addresses on Interfaces, page 24-8
- Change the Interface Delay Value, page 24-9
- Enable EIGRP Authentication on an Interface, page 24-10
- Define an EIGRP Neighbor, page 24-11
- Redistribute Routes Into EIGRP, page 24-12
- Filter Networks in EIGRP, page 24-13
- Customize the EIGRP Hello Interval and Hold Time, page 24-14
- Disable Automatic Route Summarization, page 24-15
- Configure Default Information in EIGRP, page 24-16
- Disable EIGRP Split Horizon, page 24-17
- Restart the EIGRP Process, page 24-17

Define a Network for an EIGRP Routing Process

The Network table lets you specify the networks used by the EIGRP routing process. For an interface to participate in EIGRP routing, it must fall within the range of addresses defined by the network entries. For directly connected and static networks to be advertised, they must also fall within the range of the network entries.

The Network table displays the networks configured for the EIGRP routing process. Each row of the table displays the network address and associated mask configured for the specified EIGRP routing process.

To add or define a network, perform the following steps:

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
router eigrp as-num
```

Example:
Customize EIGRP

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

Example:

```
ciscoasa(config)# router eigrp 2
```

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

You can configure one or more `network` statements with this command.

Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure Passive Interfaces, page 24-8.

Configure Interfaces for EIGRP

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, you can configure a `network` command that includes the network to which the interface is attached, and use the `passive-interface` command to prevent that interface from sending or receiving EIGRP updates.

To configure interfaces for EIGRP, perform the following steps:

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
ciscoasa(config)# router eigrp as-num
```

Example:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

```
ciscoasa(config-router)# network ip-addr [mask]
```

Example:

```
ciscoasa(config)# router eigrp 2
```

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

You can configure one or more `network` statements with this command.

Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Define a Network for an EIGRP Routing Process, page 24-5.

Step 3 Control the sending or receiving of candidate default route information:

```
no default-information {in | out | WORD}
```
Customize EIGRP

Example:

ciscoasa(config)# router eigrp 2

ciscoasa(config-router)# network 10.0.0.0 255.0.0.0

ciscoasa(config-router)# no default-information (in | out | WORD)

Entering the **no default-information in** command causes the candidate default route bit to be blocked on received routes.

Entering the **no default-information out** command disables the setting of the default route bit in advertised routes.

For more information see, **Configure Default Information in EIGRP, page 24-16.**

**Step 4**

Enable MD5 authentication of EIGRP packets:

```
authentication mode eigrp as-num md5
```

Example:

ciscoasa(config)# authentication mode eigrp 2 md5

The *as-num* argument is the autonomous system number of the EIGRP routing process configured on the ASA. If EIGRP is not enabled or if you enter the wrong number, the ASA returns the following error message:

```
% Asystem(100) specified does not exist
```

For more information see **Enable EIGRP Authentication on an Interface, page 24-10.**

**Step 5**

Set the delay value:

```
delay value
```

Example:

ciscoasa(config-if)# delay 200

The *value* argument entered is in tens of microseconds. To set the delay for 2000 microseconds, you enter a *value* of 200.

To view the delay value assigned to an interface, use the **show interface** command.

For more information see **Change the Interface Delay Value, page 24-9.**

**Step 6**

Change the hello interval:

```
hello-interval eigrp as-num seconds
```

Example:

ciscoasa(config)# hello-interval eigrp 2 60

For more information see **Customize the EIGRP Hello Interval and Hold Time, page 24-14.**

**Step 7**

Change the hold time:

```
hold-time eigrp as-num seconds
```

Example:

ciscoasa(config)# hold-time eigrp 2 60

For more information see **Customize the EIGRP Hello Interval and Hold Time, page 24-14.**
Configure Passive Interfaces

You can configure one or more interfaces as passive interfaces. In EIGRP, a passive interface does not send or receive routing updates. To configure passive interfaces, perform the following steps:

Procedure

Step 1  Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
router eigrp  as-num
```

Example:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

Step 2  Configure the interfaces and networks that participate in EIGRP routing. You can configure one or more `network` statements with this command:

```
ciscoasa(config-router)# network  ip-addr [mask]
```

Example:

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Define a Network for an EIGRP Routing Process, page 24-5.

Step 3  Prevent an interface from sending or receiving EIGRP routing messages:

```
passive-interface  {default  |  if-name}
```

Example:

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Using the `default` keyword disables EIGRP routing updates on all interfaces. Specifying an interface name, as defined by the `nameif` command, disables EIGRP routing updates on the specified interface.

You can use multiple `passive-interface` commands in your EIGRP router configuration.

Configure the Summary Aggregate Addresses on Interfaces

You can configure summary addresses on a per-interface basis. You need to manually define summary addresses if you want to create summary addresses that do not occur at a network number boundary or if you want to use summary addresses on an ASA with automatic route summarization disabled. If any more specific routes are in the routing table, EIGRP will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes.

To create a summary address, perform the following steps:

Procedure
Step 1 Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP:

```
interface phy_if
```

Example:

```
ciscoasa(config)# interface inside
```

Step 2 Create the summary address:

```
summary-address eigrp as-num address mask [distance]
```

Example:

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

By default, EIGRP summary addresses that you define have an administrative distance of 5. You can change this value by specifying the optional `distance` argument in the `summary-address` command.

---

### Change the Interface Delay Value

The interface delay value is used in EIGRP distance calculations. You can modify this value on a per-interface basis.

To change the interface delay value, perform the following steps:

**Procedure**

---

Step 1 Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP:

```
interface phy_if
```

Example:

```
ciscoasa(config)# interface inside
```

Step 2 Set a delay value:

```
delay value
```

Example:

```
ciscoasa(config-if)# delay 200
```

The `value` argument entered is in tens of microseconds. To set the delay for 2000 microseconds, you enter a `value` of 200.

**Note** To view the delay value assigned to an interface, use the `show interface` command.
Enable EIGRP Authentication on an Interface

EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol. The MD5 keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

EIGRP route authentication is configured on a per-interface basis. All EIGRP neighbors on interfaces configured for EIGRP message authentication must be configured with the same authentication mode and key for adjacencies to be established.

Note: Before you can enable EIGRP route authentication, you must enable EIGRP.

To enable EIGRP authentication on an interface, perform the following steps:

Procedure

Step 1: Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
router eigrp as-num
```

Example:

```
hostname(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

Step 2: Configure the interfaces and networks that participate in EIGRP routing:

```
network ip-addr [mask]
```

Example:

```
hostname(config)# router eigrp 2
hostname(config-router)# network 10.0.0.0 255.0.0.0
```

- You can configure one or more network statements with this command.
- Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that falls within the defined network participate in the EIGRP routing process.
- If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure EIGRP, page 24-3.

Step 3: Enter interface configuration mode for the interface on which you are configuring EIGRP message authentication:

```
interface phy_if
```

Example:

```
hostname(config)# interface inside
```

Step 4: Enable MD5 authentication of EIGRP packets:

```
authentication mode eigrp as-num md5
```

Example:

```
hostname(config)# authentication mode eigrp 2 md5
```
The `as-num` argument is the autonomous system number of the EIGRP routing process configured on the ASA. If EIGRP is not enabled or if you enter the wrong number, the ASA returns the following error message:

```
% Asystem(100) specified does not exist
```

**Step 5** Configure the key used by the MD5 algorithm:

```
authentication key eigrp as-num key key-id key-id
```

Example:

```
hostname(config)# authentication key eigrp 2 cisco key-id 200
```

- The `as-num` argument is the autonomous system number of the EIGRP routing process configured on the ASA. If EIGRP is not enabled or if you enter the wrong number, the ASA returns the following error message:

```
% Asystem(100) specified does not exist
```

- The `key` argument can include up to 16 characters, including alphabets, numbers and special characters. White spaces are not allowed, in the key argument.

- The `key-id` argument is a number that can range from 0 to 255.

---

**Define an EIGRP Neighbor**

EIGRP hello packets are sent as multicast packets. If an EIGRP neighbor is located across a non broadcast network, such as a tunnel, you must manually define that neighbor. When you manually define an EIGRP neighbor, hello packets are sent to that neighbor as unicast messages.

To manually define an EIGRP neighbor, perform the following steps:

**Procedure**

---

**Step 1** Create an EIGRP routing process and enters router configuration mode for this EIGRP process:

```
router eigrp as-num
```

Example:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

**Step 2** Define the static neighbor:

```
neighbor ip-addr interface if_name
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

The `ip-addr` argument is the IP address of the neighbor.
Customize EIGRP

The `if-name` argument is the name of the interface, as specified by the `nameif` command, through which that neighbor is available. You can define multiple neighbors for an EIGRP routing process.

Redistribute Routes Into EIGRP

You can redistribute routes discovered by RIP and OSPF into the EIGRP routing process. You can also redistribute static and connected routes into the EIGRP routing process. You do not need to redistribute connected routes if they fall within the range of a `network` statement in the EIGRP configuration.

**Note**

For RIP only: Before you begin this procedure, you must create a route map to further define which routes from the specified routing protocol are redistributed into the RIP routing process. See Chapter 21, “Route Maps,” for more information about creating a route map.

To redistribute routes into the EIGRP routing process, perform the following steps:

**Procedure**

**Step 1** Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```plaintext
erouter eigrp as-num
```

Example:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

**Step 2** (Optional) Specifies the default metrics that should be applied to routes redistributed into the EIGRP routing process:

```plaintext
default-metric bandwidth delay reliability loading mtu
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

If you do not specify a default metric in the EIGRP router configuration, you must specify the metric values in each `redistribute` command. If you specify the EIGRP metrics in the `redistribute` command and have the `default-metric` command in the EIGRP router configuration, the metrics in the `redistribute` command are used.

**Step 3** Redistribute connected routes into the EIGRP routing process:

```plaintext
redistribute connected [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

Example:

```
ciscoasa(config-router): redistribute connected [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

You must specify the EIGRP metric values in the `redistribute` command if you do not have a `default-metric` command in the EIGRP router configuration.
**Chapter 24 EIGRP**

**Customize EIGRP**

**Step 4**  
Redistribute static routes into the EIGRP routing process:

```
redistribute static [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

Example:

```
ciscoasa(config-router): redistribute static [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

**Step 5**  
Redistribute routes from an OSPF routing process into the EIGRP routing process:

```
redistribute ospf pid [match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

Example:

```
ciscoasa(config-router): redistribute ospf pid [match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

**Step 6**  
Redistribute routes from a RIP routing process into the EIGRP routing process:

```
redistribute rip [metric bandwidth delay reliability load mtu] [route-map map_name]
```

Example:

```
(config-router): redistribute rip [metric bandwidth delay reliability load mtu] [route-map map_name]
```

---

**Filter Networks in EIGRP**

**Note**  
Before you begin this process, you must create a standard ACL that defines the routes that you want to advertise. That is, create a standard ACL that defines the routes that you want to filter from sending or receiving updates.

To filter networks in EIGRP, perform the following steps:

**Procedure**

**Step 1**  
Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
router eigrp as-num
```

Example:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

**Step 2**  
Configure the interfaces and networks that participate in EIGRP routing:

```
ciscoasa(config-router)# network ip-addr [mask]
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```
You can configure one or more network statements with this command.

Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure Interfaces for EIGRP, page 24-6.

**Step 3** Filter networks sent in EIGRP routing updates:

```
distribute-list acl out [connected | ospf | rip | static | interface if_name]
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl out [connected]
```

You can specify an interface to apply the filter to only those updates that are sent by that specific interface.

You can enter multiple `distribute-list` commands in your EIGRP router configuration.

**Step 4** Filter networks received in EIGRP routing updates:

```
distribute-list acl in [interface if_name]
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl in [interface interface1]
```

You can specify an interface to apply the filter to only those updates that are received by that interface.

---

**Customize the EIGRP Hello Interval and Hold Time**

The ASA periodically sends hello packets to discover neighbors and to learn when neighbors become unreachable or inoperative. By default, hello packets are sent every 5 seconds.

The hello packet advertises the ASA hold time. The hold time indicates to EIGRP neighbors the length of time the neighbor should consider the ASA reachable. If the neighbor does not receive a hello packet within the advertised hold time, then the ASA is considered unreachable. By default, the advertised hold time is 15 seconds (three times the hello interval).

Both the hello interval and the advertised hold time are configured on a per-interface basis. We recommend setting the hold time to be at minimum three times the hello interval.

To configure the hello interval and advertised hold time, perform the following steps:

**Procedure**

**Step 1** Enter interface configuration mode for the interface on which you are configuring the hello interval or advertised hold time:
interface phy_if

Example:
ciscoasa(config)# interface inside

Step 2  Change the hello interval:
hello-interval eigrp as-num seconds

Example:
ciscoasa(config)# hello-interval eigrp 2 60

Step 3  Change the hold time:
hold-time eigrp as-num seconds

Example:
ciscoasa(config)# hold-time eigrp 2 60

Disable Automatic Route Summarization

Automatic route summarization is enabled by default. The EIGRP routing process summarizes on network number boundaries. This can cause routing problems if you have noncontiguous networks.

For example, if you have a router with the networks 192.168.1.0, 192.168.2.0, and 192.168.3.0 connected to it, and those networks all participate in EIGRP, the EIGRP routing process creates the summary address 192.168.0.0 for those routes. If an additional router is added to the network with the networks 192.168.10.0 and 192.168.11.0, and those networks participate in EIGRP, they will also be summarized as 192.168.0.0. To prevent the possibility of traffic being routed to the wrong location, you should disable automatic route summarization on the routers creating the conflicting summary addresses.

Procedure

Step 1  Create an EIGRP routing process and enter router configuration mode for this EIGRP process:
router eigrp as-num

Example:
ciscoasa(config)# router eigrp 2

The as-num argument is the autonomous system number of the EIGRP routing process.

Step 2  Disable automatic route summarization:
no auto-summary

Example:
ciscoasa(config-router)# no auto-summary

Automatic summary addresses have a default administrative distance of 5.
Configure Default Information in EIGRP

You can control the sending and receiving of default route information in EIGRP updates. By default, default routes are sent and accepted. Configuring the ASA to disallow default information to be received causes the candidate default route bit to be blocked on received routes. Configuring the ASA to disallow default information to be sent disables the setting of the default route bit in advertised routes.

Procedure

**Step 1** Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

```
router eigrp as-num
```

Example:

```
ciscoasa(config)# router eigrp 2
```

The `as-num` argument is the autonomous system number of the EIGRP routing process.

**Step 2** Configure the interfaces and networks that participate in EIGRP routing:

```
network ip-addr [mask]
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

You can configure one or more network statements with this command. Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure Interfaces for EIGRP, page 24-6.

**Step 3** Control the sending or receiving of candidate default route information:

```
no default-information {in | out | WORD}
```

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

**Note** Entering the `no default-information in` command causes the candidate default route bit to be blocked on received routes. Entering the `no default-information out` command disables the setting of the default route bit in advertised routes.
Disable EIGRP Split Horizon

Split horizon controls the sending of EIGRP update and query packets. When split horizon is enabled on an interface, update and query packets are not sent for destinations for which this interface is the next hop. Controlling update and query packets in this manner reduces the possibility of routing loops.

By default, split horizon is enabled on all interfaces.

Split horizon blocks route information from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routing devices, particularly when links are broken. However, with nonbroadcast networks, there may be situations where this behavior is not desired. For these situations, including networks in which you have EIGRP configured, you may want to disable split horizon.

If you disable split horizon on an interface, you must disable it for all routers and access servers on that interface.

To disable EIGRP split horizon, perform the following steps:

Procedure

---

**Step 1**
Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP:

`interface phy_if`

Example:

```
ciscoasa(config)# interface phy_if
```

**Step 2**
Disable the split horizon:

`no split-horizon eigrp as-number`

Example:

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

---

Restart the EIGRP Process

You can restart an EIGRP process or clear redistribution or clear counters.

Procedure

---

**Step 1**
Restart an EIGRP process or clear redistribution or clear counters:

`clear eigrp pid (1-65535 | neighbors | topology | events)`

Example:

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```
Monitoring for EIGRP

You can use the following commands to monitor the EIGRP routing process. For examples and descriptions of the command output, see the command reference. Additionally, you can disable the logging of neighbor change messages and neighbor warning messages.

To monitor or disable various EIGRP routing statistics, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router-id</code></td>
<td>Displays the router-id for this EIGRP process.</td>
</tr>
<tr>
<td>`show eigrp [as-number] events {(start end)</td>
<td>type}`</td>
</tr>
<tr>
<td><code>show eigrp [as-number] interfaces [if-name] {detail}</code></td>
<td>Displays the interfaces participating in EIGRP routing.</td>
</tr>
<tr>
<td>`show eigrp [as-number] neighbors {detail</td>
<td>static} [if-name]`</td>
</tr>
<tr>
<td>`show eigrp [as-number] topology {ip-addr</td>
<td>mask</td>
</tr>
<tr>
<td><code>show eigrp [as-number] traffic</code></td>
<td>Displays EIGRP traffic statistics.</td>
</tr>
<tr>
<td><code>show mfib cluster</code></td>
<td>Displays MFIB information in terms of forwarding entries and interfaces.</td>
</tr>
<tr>
<td><code>show route cluster</code></td>
<td>Displays additional route synchronization details for clustering.</td>
</tr>
</tbody>
</table>

Disabling EIGRP Logging Messages

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no eigrp log-neighbor-changes</code></td>
<td>Disables the logging of neighbor change messages. Enter this command in router configuration mode for the EIGRP routing process.</td>
</tr>
<tr>
<td><code>no eigrp log-neighbor-warnings</code></td>
<td>Disables the logging of neighbor warning messages.</td>
</tr>
</tbody>
</table>

By default, neighbor change and neighbor warning messages are logged.

**Example for EIGRP**

The following example shows how to enable and configure EIGRP with various optional processes:

**Step 1**

To enable EIGRP, enter the following commands:

```
ciscoasa(config)# router eigrp 2
```
```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```
Step 2  To configure an interface from sending or receiving EIGRP routing messages, enter the following command:

```
ciscoasa(config-router)# passive-interface (default)
```

Step 3  To define an EIGRP neighbor, enter the following command:

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

Step 4  To configure the interfaces and networks that participate in EIGRP routing, enter the following command:

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Step 5  To change the interface delay value used in EIGRP distance calculations, enter the following commands:

```
ciscoasa(config-router)# exit

ciscoasa(config)# interface phy_if

ciscoasa(config-if)# delay 200
```

## History for EIGRP

### Table 24-1  Feature History for EIGRP

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| EIGRP Support             | 7.0(1)            | Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the Enhanced Interior Gateway Routing Protocol (EIGRP).
|                           |                   | We introduced the following command: `route eigrp`.                                                                                                      |
| Dynamic Routing in Multiple Context Mode | 9.0(1)            | EIGRP routing is supported in multiple context mode.                                                                                                    |
| Clustering                | 9.0(1)            | For EIGRP, bulk synchronization, route synchronization, and layer 2 load balancing are supported in the clustering environment.                      |
|                           |                   | We introduced or modified the following commands: `show route cluster`, `debug route cluster`, `show mfib cluster`, `debug mfib cluster`.          |
| EIGRP Auto-Summary        | 9.2(1)            | For EIGRP, the Auto-Summary field is now disabled by default.                                                                                           |
Multicast Routing

This chapter describes how to configure the Cisco ASA to use the multicast routing protocol.

- About Multicast Routing, page 25-1
- Guidelines for Multicast Routing, page 25-3
- Enable Multicast Routing, page 25-3
- Customize Multicast Routing, page 25-4
- Example for Multicast Routing, page 25-15
- History for Multicast Routing, page 25-16

About Multicast Routing

Multicast routing is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast routing include videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

Multicast routing protocols delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by Cisco routers enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols resulting in the most efficient delivery of data to multiple receivers possible.

The ASA supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single ASA.

Note

The UDP and non-UDP transports are both supported for multicast routing. However, the non-UDP transport has no FastPath optimization.

- Stub Multicast Routing, page 25-2
- PIM Multicast Routing, page 25-2
- Multicast Group Concept, page 25-2
- Clustering, page 25-2
Stub Multicast Routing

Stub multicast routing provides dynamic host registration and facilitates multicast routing. When configured for stub multicast routing, the ASA acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the ASA forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for stub multicast routing, the ASA cannot be configured for PIM.

The ASA supports both PIM-SM and bidirectional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a single Rendezvous Point per multicast group and optionally creates shortest-path trees per multicast source.

PIM Multicast Routing

Bi-directional PIM is a variant of PIM-SM that builds bi-directional shared trees connecting multicast sources and receivers. Bi-directional trees are built using a DF election process operating on each link of the multicast topology. With the assistance of the DF, multicast data is forwarded from sources to the Rendezvous Point, and therefore along the shared tree to receivers, without requiring source-specific state. The DF election takes place during Rendezvous Point discovery and provides a default route to the Rendezvous Point.

Note

If the ASA is the PIM Rendezvous Point, use the untranslated outside address of the ASA as the Rendezvous Point address.

Multicast Group Concept

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group using IGMP. Hosts must be a member of the group to receive the data stream.

Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

Clustering

Multicast routing supports clustering. In Layer 2 clustering, the master unit sends all multicast routing packets and data packets until fast-path forwarding is established. After fast-path forwarding is established, slave units may forward multicast data packets. All data flows are full flows. Stub forwarding flows are also supported. Because only one unit receives multicast packets in Layer 2...
clustering, redirection to the master unit is common. In Layer 3 clustering, units do not act independently. All data and routing packets are processed and forwarded by the master unit. Slave units drop all packets that have been sent.

For more information about clustering, see Chapter 8, “ASA Cluster.”

### Guidelines for Multicast Routing

#### Context Mode Guidelines
Supported in single context mode. In multiple context mode, unshared interfaces and shared interfaces are not supported.

#### Firewall Mode Guidelines
Supported only in routed firewall mode. Transparent firewall mode is not supported.

#### IPv6 Guidelines
Does not support IPv6.

#### Additional Guidelines
In clustering, for IGMP and PIM, this feature is only supported on the master unit.

### Enable Multicast Routing

Enabling multicast routing on the ASA, enables IGMP and PIM on all interfaces by default. IGMP is used to learn whether members of a group are present on directly attached subnets. Hosts join multicast groups by sending IGMP report messages. PIM is used to maintain forwarding tables to forward multicast datagrams.

**Note**

Only the UDP transport layer is supported for multicast routing.

#### Procedure

**Step 1**
Enable multicast routing:

```
multicast-routing
```

Example:

```
ciscoasa(config)# multicast-routing
```

The number of entries in the multicast routing tables are limited by the amount of RAM on the ASA.
Table 25-1 lists the maximum number of entries for specific multicast tables based on the amount of RAM on the ASA. Once these limits are reached, any new entries are discarded.

<table>
<thead>
<tr>
<th>Table</th>
<th>16 MB</th>
<th>128 MB</th>
<th>128+ MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFIB</td>
<td>1000</td>
<td>3000</td>
<td>30000</td>
</tr>
<tr>
<td>IGMP Groups</td>
<td>1000</td>
<td>3000</td>
<td>30000</td>
</tr>
<tr>
<td>PIM Routes</td>
<td>3000</td>
<td>7000</td>
<td>72000</td>
</tr>
</tbody>
</table>

Customize Multicast Routing

This section describes how to customize multicast routing.

- Configure Stub Multicast Routing and Forward IGMP Messages, page 25-4
- Configure a Static Multicast Route, page 25-5
- Configure IGMP Features, page 25-5
- Configure PIM Features, page 25-10
- Configure a Bidirectional Neighbor Filter, page 25-14
- Configure a Multicast Boundary, page 25-15

Configure Stub Multicast Routing and Forward IGMP Messages

Note
Stub multicast routing and PIM are not supported concurrently.

An ASA acting as the gateway to the stub area does not need to participate in PIM. Instead, you can configure it to act as an IGMP proxy agent and forward IGMP messages from hosts connected on one interface to an upstream multicast router on another interface. To configure the ASA as an IGMP proxy agent, forward the host join and leave messages from the stub area interface to an upstream interface.

Procedure

Step 1
Configure stub multicast routing and forward IGMP messages:

```
igmp forward interface if_name
```

Example:

```
ciscoasa(config-if)# igmp forward interface interface1
```
Configure a Static Multicast Route

Configuring static multicast routes lets you separate multicast traffic from unicast traffic. For example, when a path between a source and destination does not support multicast routing, the solution is to configure two multicast devices with a GRE tunnel between them and to send the multicast packets over the tunnel.

When using PIM, the ASA expects to receive packets on the same interface where it sends unicast packets back to the source. In some cases, such as bypassing a route that does not support multicast routing, you may want unicast packets to take one path and multicast packets to take another.

Static multicast routes are not advertised or redistributed.

Procedure

Step 1
Configure a static multicast route:
\[ \text{mroute src_ip src_mask (input_if_name | rpf_neighbor) [distance]} \]

Example:
ciscoasa(config)# mroute src_ip src_mask (input_if_name | rpf_neighbor) [distance]

Step 2
Configure a static multicast route for a stub area:
\[ \text{mroute src_ip src_mask input_if_name [dense output_if_name] [distance]} \]

Example:
ciscoasa(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]

The dense output_if_name keyword and argument pair is only supported for stub multicast routing.

Configure IGMP Features

IP hosts use the Internet Group Management Protocol (IGMP) to report their group memberships to directly connected multicast routers.

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP uses group addresses (Class D IP address) as group identifiers. Host group address can be in the range of 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is never assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

When you enable multicast routing on the ASA, IGMP Version 2 is automatically enabled on all interfaces.
Customize Multicast Routing

Chapter 25      Multicast Routing

Only the **no igmp** command appears in the interface configuration when you use the **show run** command. If the **multicast-routing** command appears in the device configuration, then IGMP is automatically enabled on all interfaces.

This section describes how to configure optional IGMP setting on a per-interface basis.

- **Disable IGMP on an Interface, page 25-6**
- **Configure IGMP Group Membership, page 25-6**
- **Configure a Statically Joined IGMP Group, page 25-7**
- **Control Access to Multicast Groups, page 25-7**
- **Limit the Number of IGMP States on an Interface, page 25-8**
- **Modify the Query Messages to Multicast Groups, page 25-9**
- **Change the IGMP Version, page 25-10**

**Disable IGMP on an Interface**

You can disable IGMP on specific interfaces. This information is useful if you know that there are no multicast hosts on a specific interface and you want to prevent the ASA from sending host query messages on that interface.

**Procedure**

**Step 1**

Disable IGMP on an interface:

\[ \text{no igmp} \]

Example:

\[ \text{ciscoasa(config-if)# no igmp} \]

To reenable IGMP on an interface, use the **igmp** command.

**Note**

Only the **no igmp** command appears in the interface configuration.

**Configure IGMP Group Membership**

You can configure the ASA to be a member of a multicast group. Configuring the ASA to join a multicast group causes upstream routers to maintain multicast routing table information for that group and keep the paths for that group active.

**Note**

If you want to forward multicast packets for a specific group to an interface without the ASA accepting those packets as part of the group, see **Configure a Statically Joined IGMP Group, page 25-7**.
Chapter 25  Multicast Routing

Customize Multicast Routing

Procedure

**Step 1**
Configure the ASA to be a member of a multicast group:

```
igmp join-group group-address
```

Example:
```
ciscoasa(config-if)# igmp join-group mcast-group
```

The *group-address* argument is the IP address of the group.

### Configure a Statically Joined IGMP Group

Sometimes a group member cannot report its membership in the group because of some configuration, or there may be no members of a group on the network segment. However, you still want multicast traffic for that group to be sent to that network segment. You can have multicast traffic for that group sent to the segment by configuring a statically joined IGMP group.

Enter the `igmp static-group` command. The ASA does not accept the multicast packets, but instead forwards them to the specified interface.

**Procedure**

**Step 1**
Configure the ASA statically to join a multicast group on an interface:

```
igmp static-group
```

Example:
```
ciscoasa(config-if)# igmp static-group group-address
```

The *group-address* argument is the IP address of the group.

### Control Access to Multicast Groups

You can control access to multicast groups by using access control lists.

**Procedure**

**Step 1**
Create a standard ACL for the multicast traffic:

```
access-list name standard [permit | deny] ip_addr mask
```

Example:
```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

You can create more than one entry for a single ACL. You can use extended or standard ACLs.
Customize Multicast Routing

Step 2

Create an extended ACL:

```bash
access-list name extended [permit | deny] protocol src_ip_addr src_mask dst_ip_addr dst_mask
```

Example:

```bash
ciscoasa(config)# access-list acl2 extended permit protocol src_ip_addr src_mask dst_ip_addr dst_mask
```

The `dst_ip_addr` argument is the IP address of the multicast group being permitted or denied.

Step 3

Apply the ACL to an interface:

```bash
igmp access-group acl
```

Example:

```bash
ciscoasa(config-if)# igmp access-group acl
```

The `acl` argument is the name of a standard or extended IP ACL.

Limit the Number of IGMP States on an Interface

You can limit the number of IGMP states resulting from IGMP membership reports on a per-interface basis. Membership reports exceeding the configured limits are not entered in the IGMP cache, and traffic for the excess membership reports is not forwarded.

Procedure:

Step 1

Limit the number of IGMP states on an interface:

```bash
igmp limit number
```

Example:

```bash
ciscoasa(config-if)# igmp limit 50
```

Valid values range from 0 to 500, with 500 being the default value.

Setting this value to 0 prevents learned groups from being added, but manually defined memberships (using the `igmp join-group` and `igmp static-group` commands) are still permitted. The `no` form of this command restores the default value.
Modify the Query Messages to Multicast Groups

The ASA sends query messages to discover which multicast groups have members on the networks attached to the interfaces. Members respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Query messages are addressed to the all-systems multicast group, which has an address of 224.0.0.1, with a time-to-live value of 1.

These messages are sent periodically to refresh the membership information stored on the ASA. If the ASA discovers that there are no local members of a multicast group still attached to an interface, it stops forwarding multicast packet for that group to the attached network, and it sends a prune message back to the source of the packets.

By default, the PIM designated router on the subnet is responsible for sending the query messages. By default, they are sent once every 125 seconds.

When changing the query response time, by default, the maximum query response time advertised in IGMP queries is 10 seconds. If the ASA does not receive a response to a host query within this amount of time, it deletes the group.

**Note**
The `igmp query-timeout` and `igmp query-interval` commands require IGMP Version 2.

To change the query interval, query response time, and query timeout value, perform the following steps:

**Procedure**

**Step 1**
Set the query interval time in seconds:

```
igmp query-interval seconds
```

Example:

```
ciscoasa(config-if)# igmp query-interval 30
```

Valid values range from 0 to 500; 125 is the default value.

If the ASA does not hear a query message on an interface for the specified timeout value (by default, 255 seconds), then the ASA becomes the designated router and starts sending the query messages.

**Step 2**
Change the timeout value of the query:

```
igmp query-timeout seconds
```

Example:

```
ciscoasa(config-if)# igmp query-timeout 30
```

Valid values range from 0 to 500; 225 is the default value.

**Step 3**
Change the maximum query response time:

```
igmp query-max-response-time seconds
```

Example:

```
ciscoasa(config-if)# igmp query-max-response-time 30
```

**Step 4**
**Change the IGMP Version**

By default, the ASA runs IGMP Version 2, which enables several additional features such as the `igmp query-timeout` and `igmp query-interval` commands.

All multicast routers on a subnet must support the same version of IGMP. The ASA does not automatically detect Version 1 routers and switch to Version 1. However, a mix of IGMP Version 1 and 2 hosts on the subnet works; the ASA running IGMP Version 2 works correctly when IGMP Version 1 hosts are present.

To control which version of IGMP is running on an interface, perform the following steps.

**Procedure**

**Step 1** Control the version of IGMP that you want to run on the interface:

```plaintext
igmp version (1 | 2)
```

Example:

```
ciscoasa(config-if)# igmp version 2
```

**Configure PIM Features**

Routers use PIM to maintain forwarding tables for forwarding multicast diagrams. When you enable multicast routing on the ASA, PIM and IGMP are automatically enabled on all interfaces.

*Note* PIM is not supported with PAT. The PIM protocol does not use ports, and PAT only works with protocols that use ports.

This section describes how to configure optional PIM settings.

- Enable and Disable PIM on an Interface, page 25-10
- Configure a Static Rendezvous Point Address, page 25-11
- Configure the Designated Router Priority, page 25-12
- Configure and Filter PIM Register Messages, page 25-12
- Configure PIM Message Intervals, page 25-12
- Filter PIM Neighbors, page 25-13

**Enable and Disable PIM on an Interface**

You can enable or disable PIM on specific interfaces. To enable or disable PIM on an interface, perform the following steps:

**Procedure**

**Step 1** Enable or reenable PIM on a specific interface:
Chapter 25      Multicast Routing

Customize Multicast Routing

```
pim
```

Example:
```
ciscoasa(config-if)# pim
```

**Step 2**  
Disable PIM on a specific interface:
```
no pim
```

Example:
```
ciscoasa(config-if)# no pim
```

**Note**  
Only the `no pim` command appears in the interface configuration.

---

**Configure a Static Rendezvous Point Address**

All routers within a common PIM sparse mode or bidir domain require knowledge of the PIM RP address. The address is statically configured using the `pim rp-address` command.

**Note**  
The ASA does not support Auto-RP or PIM BSR. You must use the `pim rp-address` command to specify the RP address.

You can configure the ASA to serve as RP to more than one group. The group range specified in the ACL determines the PIM RP group mapping. If an ACL is not specified, then the RP for the group is applied to the entire multicast group range (224.0.0.0/4).

To configure the address of the PIM PR perform the following steps.

**Procedure**

**Step 1**  
Enable or reenable PIM on a specific interface:
```
pim rp-address ip_address [acl] [bidir]
```

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

The `ip_address` argument is the unicast IP address of the router assigned to be a PIM RP.

The `acl` argument is the name or number of a standard ACL that defines with which multicast groups the RP should be used. Do not use a host ACL with this command.

Excluding the `bidir` keyword causes the groups to operate in PIM sparse mode.

**Note**  
The ASA always advertises the bidirectional capability in the PIM hello messages, regardless of the actual bidirectional configuration.
**Configure the Designated Router Priority**

The DR is responsible for sending PIM register, join, and prune messages to the RP. When there is more than one multicast router on a network segment, selecting the DR is based on the DR priority. If multiple devices have the same DR priority, then the device with the highest IP address becomes the DR.

By default, the ASA has a DR priority of 1. To change this value perform the following steps:

**Procedure**

**Step 1** Change the designated router priority:

```
pim dr-priority num
```

Example:
```
ciscoasa(config-if)# pim dr-priority 500
```

The `num` argument can be any number ranging from 1 to 4294967294.

**Configure and Filter PIM Register Messages**

When the ASA is acting as an RP, you can restrict specific multicast sources from registering with it to prevent unauthorized sources from registering with the RP. The Request Filter pane lets you define the multicast sources from which the ASA will accept PIM register messages.

To filter PIM register messages perform the following steps:

**Procedure**

**Step 1** Configure the ASA to filter PIM register messages:

```
pim accept-register {list acl | route-map map-name}
```

Example:
```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

In the example, the ASA filters PIM register messages `acl1` and route map `map2`.

**Configure PIM Message Intervals**

Router query messages are used to select the PIM DR. The PIM DR is responsible for sending router query messages. By default, router query messages are sent every 30 seconds. Additionally, every 60 seconds, the ASA sends PIM join or prune messages.

To change these intervals, perform the following steps:

**Procedure**
Step 1  Send router query messages:

```
pim hello-interval seconds
```

Example:
```
ciscoasa(config-if)# pim hello-interval 60
```

Valid values for the `seconds` argument range from 1 to 3600 seconds.

Step 2  Change the amount of time (in seconds) that the ASA sends PIM join or prune messages:

```
pim join-prune-interval seconds
```

Example:
```
ciscoasa(config-if)# pim join-prune-interval 60
```

Valid values for the `seconds` argument range from 10 to 600 seconds.

---

**Filter PIM Neighbors**

You can define the routers that can become PIM neighbors. By filtering the routers that can become PIM neighbors, you can do the following:

- Prevent unauthorized routers from becoming PIM neighbors.
- Prevent attached stub routers from participating in PIM.

To define neighbors that can become a PIM neighbor, perform the following steps:

**Procedure**

**Step 1**  Use a standard ACL to define the routers that you want to have participate in PIM:

```
access-list pim_nbr deny router-IP_addr PIM neighbor
```

Example:
```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

In the example, the following ACL, when used with the `pim neighbor-filter` command, prevents the 10.1.1.1 router from becoming a PIM neighbor.

**Step 2**  Filter neighbor routers:

```
pim neighbor-filter pim_nbr
```

Example:
```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

In the example, the 10.1.1.1 router is prevented from becoming a PIM neighbor on interface GigabitEthernet0/3.
Configure a Bidirectional Neighbor Filter

The Bidirectional Neighbor Filter pane shows the PIM bidirectional neighbor filters, if any, that are configured on the ASA. A PIM bidirectional neighbor filter is an ACL that defines the neighbor devices that can participate in the DF election. If a PIM bidirectional neighbor filter is not configured for an interface, then there are no restrictions. If a PIM bidirectional neighbor filter is configured, only those neighbors permitted by the ACL can participate in the DF election process.

When a PIM bidirectional neighbor filter configuration is applied to the ASA, an ACL appears in the running configuration with the name `interface-name_multicast`, in which the `interface-name` is the name of the interface to which the multicast boundary filter is applied. If an ACL with that name already exists, a number is appended to the name (for example, `inside_multicast_1`). This ACL defines which devices can become PIM neighbors of the ASA.

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled for bidir to elect a DF.

The PIM bidirectional neighbor filters enable the transition from a sparse-mode-only network to a bidir network by letting you specify the routers that should participate in the DF election, while still allowing all routers to participate in the sparse-mode domain. The bidir-enabled routers can elect a DF from among themselves, even when there are non-bidir routers on the segment. Multicast boundaries on the non-bidir routers prevent PIM messages and data from the bidir groups from leaking in or out of the bidir subset cloud.

When a PIM bidirectional neighbor filter is enabled, the routers that are permitted by the ACL are considered to be bidirectionally capable. Therefore, the following is true:

- If a permitted neighbor does not support bidir, then the DF election does not occur.
- If a denied neighbor supports bidir, then the DF election does not occur.
- If a denied neighbor does not support bidir, the DF election can occur.

To define the neighbors that can become a PIM bidirectional neighbor filter, perform the following steps:

**Procedure**

**Step 1** Use a standard ACL to define the routers that you want to have participate in PIM:

```
access-list pim_nbr deny router-IP_addr PIM neighbor
```

Example:

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

In the example, the following ACL, when used with the `pim neighbor-filter` command, prevents the 10.1.1.1 router from becoming a PIM neighbor.

**Step 2** Filter neighbor routers:

```
pim bidirectional-neighbor-filter pim_nbr
```

Example:

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```
Configure a Multicast Boundary

Address scoping defines domain boundaries so that domains with RPs that have the same IP address do not leak into each other. Scoping is performed on the subnet boundaries within large domains and on the boundaries between the domain and the Internet.

You can set up an administratively scoped boundary on an interface for multicast group addresses by entering the `multicast boundary` command. IANA has designated the multicast address range from 239.0.0.0 to 239.255.255.255 as the administratively scoped addresses. This range of addresses can be reused in domains administered by different organizations. The addresses would be considered local, not globally unique.

A standard ACL defines the range of affected addresses. When a boundary is set up, no multicast data packets are allowed to flow across the boundary from either direction. The boundary allows the same multicast group address to be reused in different administrative domains.

You can configure, examine, and filter Auto-RP discovery and announcement messages at the administratively scoped boundary on an interface for multicast group addresses by entering the `filter-autorp` keyword. Any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL are removed. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

To configure a multicast boundary perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure a multicast boundary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>multicast boundary acl [filter-autorp]</code></td>
</tr>
</tbody>
</table>

Example:

`ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]`

---

**Example for Multicast Routing**

The following example shows how to enable and configure multicast routing with various optional processes:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Enable multicast routing:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ciscoasa(config)# multicast-routing</code></td>
</tr>
</tbody>
</table>

| Step 2 | Configure a static multicast route: |
Cisco ASA Series General Operations CLI Configuration Guide

Chapter 25      Multicast Routing

History for Multicast Routing

Table 25-2  Feature History for Multicast Routing

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing support</td>
<td>7.0(1)</td>
<td>Support was added for multicast routing data, authentication, and redistribution and monitoring of routing information using the multicast routing protocol. We introduced the <strong>multicast-routing</strong> command.</td>
</tr>
<tr>
<td>Clustering support</td>
<td>9.0(1)</td>
<td>Support was added for clustering. We introduced the following commands: <strong>debug mfib cluster</strong>, <strong>show mfib cluster</strong>.</td>
</tr>
</tbody>
</table>
IPv6 Neighbor Discovery

- About IPv6 Neighbor Discovery, page 26-1
- Prerequisites for IPv6 Neighbor Discovery, page 26-4
- Guidelines for IPv6 Neighbor Discovery, page 26-4
- Defaults for IPv6 Neighbor Discovery, page 26-5
- Configure IPv6 Neighbor Discovery, page 26-6
- Monitoring IPv6 Neighbor Discovery, page 26-12
- History for IPv6 Neighbor Discovery, page 26-12

About IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the readability of a neighbor, and keep track of neighboring routers.

Nodes (hosts) use neighbor discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. Hosts also use neighbor discovery to find neighboring routers that are willing to forward packets on their behalf. In addition, nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses. When a router or the path to a router fails, a host actively searches for functioning alternates.

- Neighbor Solicitation Messages, page 26-2
- Neighbor Reachable Time, page 26-2
- Duplicate Address Detection, page 26-2
- Router Advertisement Messages, page 26-3
- Static IPv6 Neighbors, page 26-4
About IPv6 Neighbor Discovery

Neighbor Solicitation Messages

Neighbor solicitation messages (ICMPv6 Type 135) are sent on the local link by nodes attempting to discover the link-layer addresses of other nodes on the local link. The neighbor solicitation message is sent to the solicited-node multicast address. The source address in the neighbor solicitation message is the IPv6 address of the node sending the neighbor solicitation message. The neighbor solicitation message also includes the link-layer address of the source node.

After receiving a neighbor solicitation message, the destination node replies by sending a neighbor advertisement message (ICMPv6 Type 136) on the local link. The source address in the neighbor advertisement message is the IPv6 address of the node sending the neighbor advertisement message; the destination address is the IPv6 address of the node that sent the neighbor solicitation message. The data portion of the neighbor advertisement message includes the link-layer address of the node sending the neighbor advertisement message.

After the source node receives the neighbor advertisement, the source node and destination node can communicate.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. When a node wants to verifying the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link. When there is such a change, the destination address for the neighbor advertisement is the all-nodes multicast address.

Neighbor Reachable Time

The neighbor reachable time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly, however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Duplicate Address Detection

During the stateless autoconfiguration process, Duplicate Address Detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while Duplicate Address Detection is performed). Duplicate Address Detection is performed first on the new link-local address. When the link-local address is verified as unique, then Duplicate Address Detection is performed all the other IPv6 unicast addresses on the interface.

Duplicate Address Detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state. An interface returning to an administratively up state restarts Duplicate Address Detection for all of the unicast IPv6 addresses on the interface.

When a duplicate address is identified, the state of the address is set to DUPLICATE, the address is not used, and the following error message is generated:

%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. However, all configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, Duplicate Address Detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (Duplicate Address Detection is performed only on the new link-local address).

The ASA uses neighbor solicitation messages to perform Duplicate Address Detection. By default, the number of times an interface performs Duplicate Address Detection is 1.

**Router Advertisement Messages**

The Cisco ASA can participate in router advertisements so that neighboring devices can dynamically learn a default router address. Router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface of the ASA. The router advertisement messages are sent to the all-nodes multicast address.

Router advertisement messages typically include the following information:

- One or more IPv6 prefix that nodes on the local link can use to automatically configure their IPv6 addresses.
- Lifetime information for each prefix included in the advertisement.
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed.
- Default router information (whether the router sending the advertisement should be used as a default router and, if so, the amount of time (in seconds) the router should be used as a default router).
- Additional information for hosts, such as the hop limit and MTU a host should use in packets that it originates.
- The amount of time between neighbor solicitation message retransmissions on a given link.
- The amount of time a node considers a neighbor reachable.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message. Because router solicitation messages are usually sent by hosts at system startup, and the host does not have a configured unicast address, the source address in router solicitation messages is usually the unspecified IPv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the router solicitation message is used as the source address in the message. The destination address in router solicitation messages is the all-routers multicast address with a scope of the link. When a router advertisement is sent in response to a router solicitation, the destination address in the router advertisement message is the unicast address of the source of the router solicitation message.

You can configure the following settings for router advertisement messages:

- The time interval between periodic router advertisement messages.
- The router lifetime value, which indicates the amount of time IPv6 nodes should consider the ASA to be the default router.
- The IPv6 network prefixes in use on the link.
- Whether or not an interface transmits router advertisement messages.

Unless otherwise noted, the router advertisement message settings are specific to an interface and are entered in interface configuration mode.
Static IPv6 Neighbors

You can manually define a neighbor in the IPv6 neighbor cache. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Prerequisites for IPv6 Neighbor Discovery

Configure IPv6 addressing according to Configuring IPv6 Addressing, page 11-11.

Guidelines for IPv6 Neighbor Discovery

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

- The interval value is included in all IPv6 router advertisements that are sent out of this interface.
- The configured time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.
- The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the ASA is configured as a default router by using the `ipv6 nd ra-lifetime` command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.
- The `ipv6 nd prefix` command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.
- By default, prefixes configured as addresses on an interface using the `ipv6 address` command are advertised in router advertisements. If you configure prefixes for advertisement using the `ipv6 nd prefix` command, then only these prefixes are advertised.
- The `default` keyword can be used to set default parameters for all prefixes.
- A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.
- When onlink is on (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.
- When autoconfig is on (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.
- For stateless autoconfiguration to work correctly, the advertised prefix length in router advertisement messages must always be 64 bits.
- The router lifetime value is included in all IPv6 router advertisements sent out of the interface. The value indicates the usefulness of the ASA as a default router on this interface.
Setting the value to a non-zero value indicates that the ASA should be considered a default router on this interface. The non-zero value for the router lifetime value should not be less than the router advertisement interval.

The following guidelines and limitations apply for configuring a static IPv6 neighbor:

- The `ipv6 neighbor` command is similar to the `arp` command. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. These entries are stored in the configuration when the `copy` command is used to store the configuration.

- Use the `show ipv6 neighbor` command to view static entries in the IPv6 neighbor discovery cache.

- The `clear ipv6 neighbor` command deletes all entries in the IPv6 neighbor discovery cache except static entries. The `no ipv6 neighbor` command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the `no ipv6 enable` command deletes all IPv6 neighbor discovery cache entries configured for that interface except static entries (the state of the entry changes to INCMP [Incomplete]).

- Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

- The `clear ipv6 neighbor` command does not remove static entries from the IPv6 neighbor discovery cache; it only clears the dynamic entries.

- The ICMP syslogs generated are caused by a regular refresh of IPv6 neighbor entries. The ASA default timer for IPv6 neighbor entry is 30 seconds, so the ASA would generate ICMPv6 neighbor discovery and response packets about every 30 seconds. If the ASA has both failover LAN and state interfaces configured with IPv6 addresses, then every 30 seconds, ICMPv6 neighbor discovery and response packets will be generated by both ASAs for both configured and link-local IPv6 addresses. In addition, each packet will generate several syslogs (ICMP connection and local-host creation or teardown), so it may appear that constant ICMP syslogs are being generated. The refresh time for IPv6 neighbor entry is configurable on the regular data interface, but not configurable on the failover interface. However, the CPU impact for this ICMP neighbor discovery traffic is minimal.

### Defaults for IPv6 Neighbor Discovery

Table 26-1 lists the default settings for IPv6 Neighbor Discovery.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value for the neighbor solicitation transmission message interval</code></td>
<td>1000 seconds between neighbor solicitation transmissions.</td>
</tr>
<tr>
<td><code>value for the neighbor reachable time</code></td>
<td>The default is 0.</td>
</tr>
<tr>
<td><code>value for the router advertisement transmission interval</code></td>
<td>The default is 200 seconds.</td>
</tr>
<tr>
<td><code>value for the router lifetime</code></td>
<td>The default is 1800 seconds.</td>
</tr>
<tr>
<td><code>value for the number of consecutive neighbor solicitation messages sent during DAD</code></td>
<td>The default is one message.</td>
</tr>
</tbody>
</table>
Configure IPv6 Neighbor Discovery

Configure IPv6 Neighbor Discovery Parameters (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix lifetime</td>
<td>The default lifetime is 2592000 seconds (30 days), and a preferred lifetime is 604800 seconds (7 days).</td>
</tr>
<tr>
<td>on-link flag</td>
<td>The flag is on by default, which means that the prefix is used on the advertising interface.</td>
</tr>
<tr>
<td>autoconfig flag</td>
<td>The flag is on by default, which means that the prefix is used for autoconfiguration.</td>
</tr>
<tr>
<td>static IPv6 neighbor</td>
<td>Static entries are not configured in the IPv6 neighbor discovery cache.</td>
</tr>
</tbody>
</table>

Configure IPv6 Neighbor Discovery

- Enter Interface Configuration Mode, page 26-6
- Configure the Neighbor Solicitation Message Interval, page 26-7
- Configure the Neighbor Reachable Time, page 26-7
- Configure the Router Advertisement Transmission Interval, page 26-8
- Configure the Router Lifetime Value, page 26-8
- Configure DAD Settings, page 26-9
- Suppress Router Advertisement Messages, page 26-9
- Configure Address Config Flags for IPv6 DHCP Relay, page 26-10
- Configure the IPv6 Prefix in Router Advertisements, page 26-10
- Configuring a Static IPv6 Neighbor, page 26-11

Enter Interface Configuration Mode

Configure neighbor discovery settings per interface. To enter interface configuration mode, perform the following steps.

Procedure

Step 1
Enter interface configuration mode:

```
interface name
```

Example:

```
hostname(config)# interface gigabitethernet 0/0
```
Configure the Neighbor Solicitation Message Interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface perform the following steps.

**Procedure**

**Step 1** Set the interval between IPv6 neighbor solicitation retransmissions on an interface:

```
ipv6 nd ns-interval value
```

Example:
```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ns-interval 9000
```

Valid values for the `value` argument range from 1000 to 3600000 milliseconds. This information is also sent in router advertisement messages.

Configure the Neighbor Reachable Time

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, perform the following steps:

**Procedure**

**Step 1** Set the amount of time that a remote IPv6 node is reachable:

```
ipv6 nd reachable-time value
```

Example:
```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd reachable-time 1700000
```

Valid values for the `value` argument range from 0 to 3600000 milliseconds. When 0 is used for the value, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value.
Configure the Router Advertisement Transmission Interval

To configure the interval between IPv6 router advertisement transmissions on an interface, perform the following steps:

**Procedure**

**Step 1**
Set the interval between IPv6 router advertisement transmissions:

```
ipv6 nd ra-interval [msec] value
```

Example:
```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-interval 201
```

The optional `msec` keyword indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is in seconds.

Valid values for the `value` argument range from 3 to 1800 seconds or from 500 to 1800000 milliseconds if the `msec` keyword is provided.

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the ASA is configured as a default router. For more information, see Configure the Router Lifetime Value, page 26-8. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the desired value.

Configure the Router Lifetime Value

To configure the router lifetime value in IPv6 router advertisements on an interface perform the following steps.

**Procedure**

**Step 1**
Specify the length of time that nodes on the local link should consider the ASA as the default router on the link:

```
ipv6 nd ra-lifetime [msec] value
```

Example:
```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-lifetime 2000
```

- The optional `msec` keyword indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is in seconds.
- Valid values for the `value` argument range from 0 to 9000 seconds.
- Entering 0 indicates that the ASA should not be considered a default router on the selected interface.
Configure DAD Settings

To specify DAD settings on the interface, perform the following steps.

Procedure

**Step 1** Specify the uniqueness of new unicast IPv6 addresses before they are assigned and ensure that duplicate IPv6 addresses are detected in the network on a link basis:

```
ipv6 nd dad attempts value
```

Example:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd dad attempts 20
```

Valid values for the `value` argument range from 0 to 600. A zero value disables DAD processing on the specified interface.

Suppress Router Advertisement Messages

Router advertisement messages are automatically sent in response to router solicitation messages. You may want to disable these messages on any interface for which you do not want the ASA to supply the IPv6 prefix (for example, the outside interface).

To suppress the router lifetime value in IPv6 router advertisements on an interface, perform the following steps.

Procedure

**Step 1** Suppress the router lifetime value:

```
ipv6 nd suppress-ra seconds
```

Example:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd suppress-ra 900
```

The `seconds` argument specifies the validity of the ASA as a default router on this interface. Valid values range from 0 to 9000 seconds.

A zero indicates that the ASA should not be considered a default router on the specified interface.

**Note** Entering this command causes the ASA to appear as a regular IPv6 neighbor on the link and not as an IPv6 router.
Configure Address Config Flags for IPv6 DHCP Relay

You can add a flag to IPv6 router advertisements to inform IPv6 autoconfiguration clients to use DHCPv6 to obtain an IPv6 address and/or additional information such as the DNS server address.

Procedure

**Step 1**
Set the Managed Address Config flag in the IPv6 router advertisement packet:

```
ipv6 nd managed-config-flag
```

Example:

```
hostname (config-if)# ipv6 nd managed-config-flag
```

This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.

**Step 2**
Set the Other Address Config flag in the IPv6 router advertisement packet:

```
ipv6 nd other-config-flag
```

Example:

```
hostname (config-if)# ipv6 nd other-config-flag
```

This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.

Configure the IPv6 Prefix in Router Advertisements

To configure the which IPv6 prefixes are included in IPv6 router advertisements, perform the following steps:

Procedure

**Step 1**
Configure which IPv6 prefixes are included in IPv6 router advertisements:

```
ipv6 nd prefix ipv6-prefix/prefix-length | default [[[valid-lifetime preferred-lifetime] | [at valid-date preferred-date] | infinite | no-advertise | off-link | no-autoconfig]
```

Example:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

- The prefix advertisement can be used by neighboring devices to autoconfigure their interface addresses. Stateless autoconfiguration uses IPv6 prefixes provided in router advertisement messages to create the global unicast address from the link-local address.
- The **at valid-date preferred-date** syntax indicates the date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached.
Chapter 26      IPv6 Neighbor Discovery

Configure the Router Advertisement Transmission Interval

• Dates are expressed in the form date-valid-expire month-valid-expire hh:mm-valid-expire
date-prefer-expire month-prefer-expire hh:mm-prefer-expire.

• The default keyword indicates that default values are used.

• The optional infinite keyword specifies that the valid lifetime does not expire.

• The ipv6-prefix argument specifies the IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

• The optional no-advertise keyword indicates to hosts on the local link that the specified prefix is not to be used for IPv6 autoconfiguration.

• The optional no-autoconfig keyword indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.

• The optional off-link keyword indicates that the specified prefix is not used for on-link determination.

• The preferred-lifetime argument specifies the amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with infinite. The default is 604800 (7 days).

• The prefix-length argument specifies the length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

• The valid-lifetime argument specifies the amount of time that the specified IPv6 prefix is advertised as being valid. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with infinite. The default is 2592000 (30 days).

Configuring a Static IPv6 Neighbor

To configure a static entry in the IPv6 neighbor discovery cache, perform the following steps:

Procedure

Step 1 Configure a static entry in the IPv6 neighbor discovery cache:

ipv6 neighbor ipv6_address if_name mac_address

Example:

hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472

The ipv6_address argument is the link-local IPv6 address of the neighbor, the if_name argument is the interface through which the neighbor is available, and the mac_address argument is the MAC address of the neighbor interface.
Monitoring IPv6 Neighbor Discovery

To monitor IPv6 neighbor discovery parameters, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 interface</td>
<td>Displays the usability status of interfaces configured for IPv6. Including the interface name, such as “outside” and displays the settings for the specified interface. Excludes the name from the command and displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following:</td>
</tr>
<tr>
<td></td>
<td>• The name and status of the interface.</td>
</tr>
<tr>
<td></td>
<td>• The link-local and global unicast addresses.</td>
</tr>
<tr>
<td></td>
<td>• The multicast groups to which the interface belongs.</td>
</tr>
<tr>
<td></td>
<td>• ICMP redirect and error message settings.</td>
</tr>
<tr>
<td></td>
<td>• Neighbor discovery settings.</td>
</tr>
<tr>
<td></td>
<td>• The actual time when the command is set to 0.</td>
</tr>
<tr>
<td></td>
<td>• The neighbor discovery reachable time that is being used.</td>
</tr>
</tbody>
</table>

History for IPv6 Neighbor Discovery

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Neighbor Discovery</td>
<td>7.0(1)</td>
<td>We introduced this feature. We introduced the following commands: ipv6 nd ns-interval, ipv6 nd ra-lifetime, ipv6 nd suppress-ra, ipv6 neighbor, ipv6 nd prefix, ipv6 nd dad-attempts, ipv6 nd reachable-time, ipv6 address, ipv6 enforce-eui64.</td>
</tr>
<tr>
<td>Address Config Flags for IPv6 DHCP Relay</td>
<td>9.0(1)</td>
<td>We introduced the following commands: ipv6 nd managed-config-flag, ipv6 nd other-config-flag.</td>
</tr>
</tbody>
</table>
PART 7

AAA Servers and the Local Database
Information About AAA

This chapter describes authentication, authorization, and accounting (AAA, pronounced “triple A”). AAA is a set of services for controlling access to computer resources, enforcing policies, assessing usage, and providing the information necessary to bill for services. These processes are considered important for effective network management and security.

- Authentication, page 27-1
- Authorization, page 27-2
- Accounting, page 27-2
- Interaction Between Authentication, Authorization, and Accounting, page 27-2
- AAA Servers, page 27-2
- AAA Server Groups, page 27-2
- Local Database Support, page 27-2

Authentication

Authentication provides a way to identify a user, typically by having the user enter a valid username and valid password before access is granted. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is permitted access to the network. If the credentials do not match, authentication fails and network access is denied.

You can configure the Cisco ASA to authenticate the following items:

- All administrative connections to the ASA, including the following sessions:
  - Telnet
  - SSH
  - Serial console
  - ASDM using HTTPS
  - VPN management access
- The enable command
- Network access
- VPN access
Authorization

Authorization is the process of enforcing policies: determining what types of activities, resources, or services a user is permitted to access. After a user is authenticated, that user may be authorized for different types of access or activity.

You can configure the ASA to authorize the following items:

- Management commands
- Network access
- VPN access

Accounting

Accounting measures the resources a user consumes during access, which may include the amount of system time or the amount of data that a user has sent or received during a session. Accounting is carried out through the logging of session statistics and usage information, which is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Interaction Between Authentication, Authorization, and Accounting

You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

AAA Servers

The AAA server is a network server that is used for access control. Authentication identifies the user. Authorization implements policies that determine which resources and services an authenticated user may access. Accounting keeps track of time and data resources that are used for billing and analysis.

AAA Server Groups

If you want to use an external AAA server for authentication, authorization, or accounting, you must first create at least one AAA server group per AAA protocol and add one or more servers to each group. You identify AAA server groups by name. Each server group is specific to one type of server or service.

Local Database Support

The ASA maintains a local database that you can populate with user profiles. You can use a local database instead of AAA servers to provide user authentication, authorization, and accounting.
Local Database for AAA

This chapter describes how to configure local servers for AAA.

- About the Local Database, page 28-1
- Guidelines for the Local Database, page 28-2
- Add a User Account to the Local Database, page 28-3
- Generate a Shared Key, page 28-5
- Monitoring the Local Database, page 28-7
- History for the Local Database, page 28-7

About the Local Database

You can use the local database for the following functions:

- ASDM per-user access
- Console authentication
- Telnet and SSH authentication
- enable command authentication
  This setting is for CLI-access only and does not affect the Cisco ASDM login.
- Command authorization
  If you turn on command authorization using the local database, then the Cisco ASA refers to the
  user privilege level to determine which commands are available. Otherwise, the privilege level is not
  generally used. By default, all commands are either privilege level 0 or level 15.
- Network access authentication
- VPN client authentication

For multiple context mode, you can configure usernames in the system execution space to provide
individual logins at the CLI using the login command; however, you cannot configure any AAA rules
that use the local database in the system execution space.

Note
You cannot use the local database for network access authorization.
Guidelines for the Local Database

Fallback Support

The local database can act as a fallback method for several functions. This behavior is designed to help you prevent accidental lockout from the ASA.

When a user logs in, the servers in the group are accessed one at a time, starting with the first server that you specify in the configuration, until a server responds. If all servers in the group are unavailable, the ASA tries the local database if you have configured it as a fallback method (for management authentication and authorization only). If you do not have a fallback method, the ASA continues to try the AAA servers.

For users who need fallback support, we recommend that their usernames and passwords in the local database match their usernames and passwords on the AAA servers. This practice provides transparent fallback support. Because the user cannot determine whether a AAA server or the local database is providing the service, using usernames and passwords on AAA servers that are different than the usernames and passwords in the local database means that the user cannot be certain which username and password should be given.

The local database supports the following fallback functions:

- Console and enable password authentication—If the servers in the group are all unavailable, the ASA uses the local database to authenticate administrative access, which can also include enable password authentication.
- Command authorization—If the TACACS+ servers in the group are all unavailable, the local database is used to authorize commands based on privilege levels.
- VPN authentication and authorization—VPN authentication and authorization are supported to enable remote access to the ASA if AAA servers that normally support these VPN services are unavailable. When a VPN client of an administrator specifies a tunnel group configured to fallback to the local database, the VPN tunnel can be established even if the AAA server group is unavailable, provided that the local database is configured with the necessary attributes.

How Fallback Works with Multiple Servers in a Group

If you configure multiple servers in a server group and you enable fallback to the local database for the server group, fallback occurs when no server in the group responds to the authentication request from the ASA. To illustrate, consider this scenario:

You configure an LDAP server group with two Active Directory servers, server 1 and server 2, in that order. When the remote user logs in, the ASA attempts to authenticate to server 1.

If server 1 responds with an authentication failure (such as user not found), the ASA does not attempt to authenticate to server 2.

If server 1 does not respond within the timeout period (or the number of authentication attempts exceeds the configured maximum), the ASA tries server 2.

If both servers in the group do not respond, and the ASA is configured to fall back to the local database, the ASA tries to authenticate to the local database.

Guidelines for the Local Database

Make sure that you prevent a lockout from the ASA when using the local database for authentication or authorization.
Add a User Account to the Local Database

To add a user to the local database, perform the following steps:

Procedure

Step 1  Create the user account.

```
username username (nopassword | password password) [ privilege priv_level]
```

Example:
```
ciscoasa(config)# username exampleuser1 privilege 1
```

The `username` keyword is a string from 3 to 64 characters long, using any combination of ASCII printable characters with the exception of spaces and the question mark. The `password` keyword is a string from 3 to 32 characters long. The `privilege` keyword sets the privilege level, which ranges from 0 to 15. The default is 2. This privilege level is used with command authorization.

Caution

If you do not use command authorization (the `aaa authorization console LOCAL` command), then the default level 2 allows management access to privileged EXEC mode. If you want to limit access to privileged EXEC mode, either set the privilege level to 0 or 1, or use the `service-type` command.

The `nopassword` keyword creates a user account with no password. The `encrypted` keyword indicates that the password is encrypted. When you define a password in the `username` command, the ASA encrypts it when it saves it to the configuration for security purposes. When you enter the `show running-config` command, the `username` command does not show the actual password; it shows the encrypted password followed by the `encrypted` keyword. For example, if you enter the password “test,” the `show running-config` output would appear as something similar to the following:
```
username user1 password DLaUIAX3l78qgOB5c7iVNw== encrypted
```

The only time you would actually enter the `encrypted` keyword at the CLI is if you are cutting and pasting a configuration file for use in another ASA, and you are using the same password.

Step 2  (Optional) Configure username attributes.

```
username username attributes
```

Example:
```
ciscoasa(config)# username exampleuser1 attributes
```

The `username` argument is the username that you created in the first step.

By default, VPN users that you add with this command have no attributes or group policy association. You must configure all values explicitly using the `username attributes` command. See the VPN configuration guide for more information.

Step 3  (Optional) Configure the user level if you configured management authorization using the `aaa authorization exec` command.

```
service-type {admin | nas-prompt | remote-access}
```

Related Topics

Recover from a Lockout, page 35-25
Example:
ciscoasa(config-username)# service-type admin

The **admin** keyword allows full access to any services specified by the **aaa authentication console LOCAL** commands. The **admin** keyword is the default.

The **nas-prompt** keyword allows access to the CLI when you configure the **aaa authentication {telnet | ssh | serial} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you enable authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command (or the **login** command).

The **remote-access** keyword denies management access. You cannot use any services specified by the **aaa authentication console commands** (excluding the **serial** keyword; serial access is allowed).

**Step 4**
Enable public key authentication for SSH connections to the ASA on a per-user basis.

```
ssh authentication {pkf | publickey key [hashed]}
```

Example:
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word 'quit' on a line by itself:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAABAAMvQ+J+cDn..gMmfnUvZQ462qzOuMKQWSX1G3snUDsRD29Wx1CwUrQVca6
C8v integersjUKM6qaCuk5YeDm0+4Oj3A23QgCw4gJ2N8G11aIeI1V/76y5m28MY/x/Ss48m0A3f/6Z
PmVda3zYgykYDy7KAIp7G2q66XNgDz+iQww1eS1j9Mn5QJshIq1LkKp3xt7uXq3mQ5vGn41P8JU
---- END SSH2 PUBLIC KEY ---- quit
```

INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)"

You can specify a public key file (PKF) formatted key (the **pkf** keyword) or a Base64 key (the **publickey** keyword). For a **publickey**, the **key** is a Base64-encoded public key. You can generate the key using any SSH key generation software (such as ssh keygen) that can generate SSH-RSA raw keys (with no certificates).

For a **pkf** key, you are prompted to paste in a PKF formatted key, up to 4096 bits. Use this format for keys that are too large to paste inline in Base64 format. For example, you can generate a 4096-bit key using ssh keygen, then convert it to pkf, and use the **pkf** keyword to be prompted for the key.  

**Note**

You can use the **pkf** option with failover, but the PKF key is not automatically replicated to the standby system. You must enter the **write standby** command to synchronize the PKF key.

When you view the key on the ASA using the **show running-config username** command, the key is encrypted using a SHA-256 hash. Even if you entered the key as **pkf**, the ASA hashes the key, and shows it as a hashed **publickey**. If you need to copy the key from **show** output, specify the **publickey** type with the **hashed** keyword.
Step 5  (Optional) If you are using this username for VPN authentication, you can configure many VPN attributes for the user. See the VPN configuration guide for more information.

Examples
The following example assigns a privilege level of 15 to the admin user account:

ciscoasa(config)# username admin password password privilege 15

The following example creates a user account with no password:

ciscoasa(config)# username user34 nopassword

The following example enables management authorization, creates a user account with a password, enters username configuration mode, and specifies a service-type of nas-prompt:

   ciscoasa(config)# aaa authorization exec authentication-server
   ciscoasa(config)# username user1 password goGeOus
   ciscoasa(config)# username user1 attributes
   ciscoasa(config-username)# service-type nas-prompt

Generate a Shared Key

To generates a shared key for SSH on a Linux or Macintosh system, and import it to the perform the following steps:

Procedure

Step 1  Generate the ssh-rsa public and private keys for 4096 bits on your computer:

   jcrichton-mac:- john$ ssh-keygen -b 4096
   Generating public/private rsa key pair.
   Enter file in which to save the key (/Users/john/.ssh/id_rsa):
   /Users/john/.ssh/id_rsa already exists.
   Overwrite (y/n)? y
   Enter passphrase (empty for no passphrase): pa$$phrase
   Enter same passphrase again: pa$$phrase
   Your identification has been saved in /Users/john/.ssh/id_rsa.
   Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
   The key fingerprint is:
   c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
   The key’s randomart image is:
   +---[ RSA 4096]-----+
   | .                 |
   | o .               |
   | +... o            |
   | B.++++.           |
   | .B .+ S           |
   | = o               |
   | + . E             |
   | o o               |
   | oooo              |
   +-----------------+

Step 2  Convert the key to PKF format:

   jcrichton-mac:- john$ cd .ssh
   jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
### Generate a Shared Key

**Step 3** Copy the key to your clipboard.

**Step 4** Connect to the ASA CLI, and add the public key to your username:

```
ciscoasa(config)# username test attributes
ciscoasa(config-username)# ssh authentication pkf
```

Enter an SSH public key formatted file. End with the word 'quit' on a line by itself:

--- BEGIN SSH2 PUBLIC KEY ---
Comment: "4096-bit RSA, converted by ramona@robersma-mac from OpenSSH"

```
AAAAB3NzaC1yc2EAAAADAQABAAABAQGvq3fH4/870/Ry1zGyj/6uVx+Qs8G6OxCR40lp6nxg39bA+5vB
QymUYVDgzrX2ta/jqGqGQl5W/h8EYJLWvU+jd/9xQ79dS41niOA58+jk/2uC9//IJCrY
p5xQ0OA1SjajQxXWPQYyO/5dkg1mXZMv6mGQ02QZ/n6HV+zFpE7fOx2Iy/3Kd5j0hL
```

--- END SSH2 PUBLIC KEY ---

**Step 5** Verify the user (test) can SSH to the ASA:

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
```

The authenticity of host '10.86.118.5' (10.86.118.5)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes

The following dialog box appears for you to enter your passphrase:
Meanwhile, in the terminal session:

Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.

Monitoring the Local Database

See the following commands for monitoring the local database:

- **show aaa-server**
  
  This command shows the configured database statistics. To clear the AAA server configuration, enter the `clear aaa-server statistics` command.

- **show running-config aaa-server**
  
  This command shows the AAA server running configuration. To clear AAA server statistics, enter the `clear configure aaa-server` command.

History for the Local Database

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local database configuration for AAA</td>
<td>7.0(1)</td>
<td>Describes how to configure the local database for AAA use. We introduced the following commands: username, aaa authorization exec authentication-server, aaa authentication console LOCAL, aaa authorization exec LOCAL, service-type, aaa authentication [telnet</td>
</tr>
<tr>
<td>Support for SSH public key authentication</td>
<td>9.1(2)</td>
<td>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). We introduced the following commands: ssh authentication. Also available in 8.4(4.1); PKF key format support is only in 9.1(2).</td>
</tr>
</tbody>
</table>
RADIUS + Servers for AAA

This chapter describes how to configure RADIUS servers for AAA.

- About RADIUS Servers for AAA, page 29-1
- Guidelines for RADIUS Servers for AAA, page 29-13
- Configure RADIUS Servers for AAA, page 29-14
- Monitoring RADIUS Servers for AAA, page 29-19
- History for RADIUS Servers for AAA, page 29-20

About RADIUS Servers for AAA

The Cisco ASA supports the following RFC-compliant RADIUS servers for AAA:

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2, and 5.x
- Cisco Identity Services Engine (ISE)
- RSA RADIUS in RSA Authentication Manager 5.2, 6.1, 7.x, and 8.x.
- Microsoft

Supported Authentication Methods

The ASA supports the following authentication methods with RADIUS servers:

- PAP—for all connection types.
- CHAP and MS-CHAPv1—for L2TP-over-IPsec connections.
- MS-CHAPv2—for L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections.

Note

To enable MS-CHAPv2 as the protocol used between the ASA and the RADIUS server for a VPN connection, password management must be enabled in the tunnel group general attributes. Enabling password management generates an MS-CHAPv2 authentication request from the ASA to the RADIUS server. See the description of the password-management command for details.
If you use double authentication and enable password management in the tunnel group, then the primary and secondary authentication requests include MS-CHAPv2 request attributes. If a RADIUS server does not support MS-CHAPv2, then you can configure that server to send a non-MS-CHAPv2 authentication request by using the `no mschapv2-capable` command.

**User Authorization of VPN Connections**

The ASA can use RADIUS servers for user authorization of VPN remote access and firewall cut-through-proxy sessions using dynamic ACLs or ACL names per user. To implement dynamic ACLs, you must configure the RADIUS server to support them. When the user authenticates, the RADIUS server sends a downloadable ACL or ACL name to the ASA. Access to a given service is either permitted or denied by the ACL. The ASA deletes the ACL when the authentication session expires.

In addition to ACLs, the ASA supports many other attributes for authorization and setting of permissions for VPN remote access and firewall cut-through proxy sessions.

**Supported Sets of RADIUS Attributes**

The ASA supports the following sets of RADIUS attributes:

- Authentication attributes defined in RFC 2138.
- Accounting attributes defined in RFC 2139.
- RADIUS attributes for tunneled protocol support, defined in RFC 2868.
- Cisco IOS Vendor-Specific Attributes (VSAs), identified by RADIUS vendor ID 9.
- Cisco VPN-related VSAs, identified by RADIUS vendor ID 3076.
- Microsoft VSAs, defined in RFC 2548.
- Cisco VSA (Cisco-Priv-Level), which provides a standard 0-15 numeric ranking of privileges, with 1 being the lowest level and 15 being the highest level. A zero level indicates no privileges. The first level (login) allows privileged EXEC access for the commands available at this level. The second level (enable) allows CLI configuration privileges.

**Supported RADIUS Authorization Attributes**

Authorization refers to the process of enforcing permissions or attributes. A RADIUS server defined as an authentication server enforces permissions or attributes if they are configured. These attributes have vendor ID 3076.

Table 29-1 lists the supported RADIUS attributes that can be used for user authorization.

---

**Note**

RADIUS attribute names do not contain the cVPN3000 prefix. Cisco Secure ACS 4.x supports this new nomenclature, but attribute names in pre-4.0 ACS releases still include the cVPN3000 prefix. The ASAs enforce the RADIUS attributes based on attribute numeric ID, not attribute name.

All attributes listed in Table 29-1 are downstream attributes that are sent from the RADIUS server to the ASA except for the following attribute numbers: 146, 150, 151, and 152. These attribute numbers are upstream attributes that are sent from the ASA to the RADIUS server. RADIUS attributes 146 and 150...
are sent from the ASA to the RADIUS server for authentication and authorization requests. All four previously listed attributes are sent from the ASA to the RADIUS server for accounting start, interim-update, and stop requests. Upstream RADIUS attributes 146, 150, 151, and 152 were introduced in Version 8.4(3).

Cisco ACS 5.x and Cisco ISE do not support IPv6 framed IP addresses for IP address assignment using RADIUS authentication in Version 9.0(1).

Table 29-1   Supported RADIUS Authorization Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Hours</td>
<td>Y</td>
<td>1</td>
<td>String</td>
<td>Single</td>
<td>Name of the time range, for example, Business-hours</td>
</tr>
<tr>
<td>Access-List-Inbound</td>
<td>Y</td>
<td>86</td>
<td>String</td>
<td>Single</td>
<td>ACL ID</td>
</tr>
<tr>
<td>Access-List-Outbound</td>
<td>Y</td>
<td>87</td>
<td>String</td>
<td>Single</td>
<td>ACL ID</td>
</tr>
<tr>
<td>Address-Pools</td>
<td>Y</td>
<td>217</td>
<td>String</td>
<td>Single</td>
<td>Name of IP local pool</td>
</tr>
<tr>
<td>Allow-Network-Extension-Mode</td>
<td>Y</td>
<td>64</td>
<td>Boolean</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>Authenticated-User-Idle-Timeout</td>
<td>Y</td>
<td>50</td>
<td>Integer</td>
<td>Single</td>
<td>1-35791394 minutes</td>
</tr>
<tr>
<td>Authorization-Required</td>
<td></td>
<td>66</td>
<td>Integer</td>
<td>Single</td>
<td>0 = No 1 = Yes</td>
</tr>
<tr>
<td>Authorization-Type</td>
<td>Y</td>
<td>65</td>
<td>Integer</td>
<td>Single</td>
<td>0 = None 1 = RADIUS 2 = LDAP</td>
</tr>
<tr>
<td>Banner1</td>
<td>Y</td>
<td>15</td>
<td>String</td>
<td>Single</td>
<td>Banner string to display for Cisco VPN remote access sessions: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, and Clientless SSL</td>
</tr>
<tr>
<td>Banner2</td>
<td>Y</td>
<td>36</td>
<td>String</td>
<td>Single</td>
<td>Banner string to display for Cisco VPN remote access sessions: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, and Clientless SSL. The Banner2 string is concatenated to the Banner1 string , if configured.</td>
</tr>
<tr>
<td>Cisco-IP-Phone-Bypass</td>
<td>Y</td>
<td>51</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>Cisco-LEAP-Bypass</td>
<td>Y</td>
<td>75</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
</tbody>
</table>
### About RADIUS Servers for AAA

#### Table 29-1  
**Supported RADIUS Authorization Attributes (continued)**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
</table>
| Client Type                                | Y   | 150       | Integer     | Single                 | 1 = Cisco VPN Client (IKEv1)  
|                                            |     |           |              |                         | 2 = AnyConnect Client SSL VPN  
|                                            |     |           |              |                         | 3 = Clientless SSL VPN  
|                                            |     |           |              |                         | 4 = Cut-Through-Proxy  
|                                            |     |           |              |                         | 5 = L2TP/IPsec SSL VPN  
|                                            |     |           |              |                         | 6 = AnyConnect Client IPsec VPN (IKEv2)                                           |
| Client-Type-Version-Limiting              | Y   | 77        | String      | Single                 | IPsec VPN version number string                                                    |
| DHCP-Network-Scope                        | Y   | 61        | String      | Single                 | IP Address                                                                        |
| Extended-Authentication-On-Rekey           | Y   | 122       | Integer     | Single                 | 0 = Disabled  
|                                            |     |           |              |                         | 1 = Enabled                                                                       |
| Group-Policy                              | Y   | 25        | String      | Single                 | Sets the group policy for the remote access VPN session. For Versions 8.2.x and later, use this attribute instead of IETF-Radius-Class. You can use one of the following formats:  
|                                            |     |           |              |                         | • group policy name                                                              
|                                            |     |           |              |                         | • OU=group policy name                                                           
|                                            |     |           |              |                         | • OU=group policy name;                                                           |
| IE-Proxy-Bypass-Local                      |     | 83        | Integer     | Single                 | 0 = None  
|                                            |     |           |              |                         | 1 = Local                                                                        |
| IE-Proxy-Exception-List                   |     | 82        | String      | Single                 | New line (\n) separated list of DNS domains                                         |
| IE-Proxy-PAC-URL                           |     | 133       | String      | Single                 | PAC address string                                                                |
| IE-Proxy-Server                           |     | 80        | String      | Single                 | IP address                                                                       |
| IE-Proxy-Server-Policy                    |     | 81        | Integer     | Single                 | 1 = No Modify  
|                                            |     |           |              |                         | 2 = No Proxy                                                                      
|                                            |     |           |              |                         | 3 = Auto detect                                                                  
|                                            |     |           |              |                         | 4 = Use Concentrator Setting                                                      |
| IKE-KeepAlive-Confidence-Interval         | Y   | 68        | Integer     | Single                 | 10-300 seconds                                                                   |
| IKE-Keepalive-Retry-Interval              | Y   | 84        | Integer     | Single                 | 2-10 seconds                                                                     |
| IKE-Keep-Alives                           | Y   | 41        | Boolean     | Single                 | 0 = Disabled  
|                                            |     |           |              |                         | 1 = Enabled                                                                       |
| Intercept-DHCP-Configure-Msg              | Y   | 62        | Boolean     | Single                 | 0 = Disabled  
|                                            |     |           |              |                         | 1 = Enabled                                                                       |
| IPsec-Allow-Passwd-Store                  | Y   | 16        | Boolean     | Single                 | 0 = Disabled  
|                                            |     |           |              |                         | 1 = Enabled                                                                       |
### Table 29-1  Supported RADIUS Authorization Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
</table>
| IPsec-Authentication                        |     | 13        | Integer     | Single                 | 0 = None  
1 = RADIUS  
2 = LDAP (authorization only)  
3 = NT Domain  
4 = SDI  
5 = Internal  
6 = RADIUS with Expiry  
7 = Kerberos/Active Directory |
| IPsec-Auth-On-Rekey                         |     | 42        | Boolean     | Single                 | 0 = Disabled  
1 = Enabled |
| IPsec-Backup-Server-List                   |     | 60        | String      | Single                 | Server Addresses (space delimited) |
| IPsec-Backup-Servers                       |     | 59        | String      | Single                 | 1 = Use Client-Configured list  
2 = Disable and clear client list  
3 = Use Backup Server list |
| IPsec-Client-Firewall-Filter-Name          |     | 57        | String      | Single                 | Specifies the name of the filter to be pushed to the client as firewall policy |
| IPsec-Client-Firewall-Filter-Optional      |     | 58        | Integer     | Single                 | 0 = Required  
1 = Optional |
| IPsec-Default-Domain                       |     | 28        | String      | Single                 | Specifies the single default domain name to send to the client (1-255 characters). |
| IPsec-IKE-Peer-ID-Check                    |     | 40        | Integer     | Single                 | 1 = Required  
2 = If supported by peer certificate  
3 = Do not check |
| IPsec-IP-Compression                       |     | 39        | Integer     | Single                 | 0 = Disabled  
1 = Enabled |
| IPsec-Mode-Config                          |     | 31        | Boolean     | Single                 | 0 = Disabled  
1 = Enabled |
| IPsec-Over-UDP                             |     | 34        | Boolean     | Single                 | 0 = Disabled  
1 = Enabled |
| IPsec-Over-UDP-Port                        |     | 35        | Integer     | Single                 | 4001- 49151. The default is 10000. |
| IPsec-Required-Client-Firewall-Capability  |     | 56        | Integer     | Single                 | 0 = None  
1 = Policy defined by remote FW Are-You-There (AYT)  
2 = Policy pushed CPP  
4 = Policy from server |
| IPsec-Sec-Association                      |     | 12        | String      | Single                 | Name of the security association |
| IPsec-Split-DNS-Names                      |     | 29        | String      | Single                 | Specifies the list of secondary domain names to send to the client (1-255 characters). |
### Table 29-1  Supported RADIUS Authorization Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
</table>
| IPsec-Split-Tunneling-Policy          | Y   | 55        | Integer     | Single                 | 0 = No split tunneling  
1 = Split tunneling  
2 = Local LAN permitted                                                            |
| IPsec-Split-Tunnel-List               | Y   | 27        | String      | Single                 | Specifies the name of the network or ACL that describes the split tunnel inclusion list. |
| IPsec-Tunnel-Type                     | Y   | 30        | Integer     | Single                 | 1 = LAN-to-LAN  
2 = Remote access                                                                 |
| IPsec-User-Group-Lock                 |     | 33        | Boolean     | Single                 | 0 = Disabled  
1 = Enabled                                                                                                                                |
| IPv6-Address-Pools                    | Y   | 218       | String      | Single                 | Name of IP local pool-IPv6                                                          |
| IPv6-VPN-Filter                       | Y   | 219       | String      | Single                 | ACL value                                                                            |
| L2TP-Encryption                       |     | 21        | Integer     | Single                 | Bitmap:  
1 = Encryption required  
2 = 40 bits  
4 = 128 bits  
8 = Stateless-Req  
15= 40/128-Encr/Stateless-Req                                                     |
| L2TP-MPPC-Compression                 |     | 38        | Integer     | Single                 | 0 = Disabled  
1 = Enabled                                                                                                                                |
| Member-Of                             | Y   | 145       | String      | Single                 | Comma-delimited string, for example: Engineering, Sales  
An administrative attribute that can be used in dynamic access policies. It does not set a group policy. |
| MS-Client-Subnet-Mask                 | Y   | 63        | Boolean     | Single                 | An IP address                                                                      |
| NAC-Default-ACL                       |     | 92        | String      |                        | ACL                                                                                |
| NAC-Enable                            |     | 89        | Integer     | Single                 | 0 = No  
1 = Yes                                                                                                                                         |
| NAC-Revalidation-Timer                |     | 91        | Integer     | Single                 | 300-86400 seconds                                                                  |
| NAC-Settings                          | Y   | 141       | String      | Single                 | Name of the NAC policy                                                              |
| NAC-Status-Query-Timer                |     | 90        | Integer     | Single                 | 30-1800 seconds                                                                    |
| Perfect-Forward-Secrecy-Enable        | Y   | 88        | Boolean     | Single                 | 0 = No  
1 = Yes                                                                                                                                         |
| PPTP-Encryption                       |     | 20        | Integer     | Single                 | Bitmap:  
1 = Encryption required  
2 = 40 bits  
4 = 128 bits  
8 = Stateless-Required  
15= 40/128-Encr/Stateless-Req                                                     |
### Table 29-1  Supported RADIUS Authorization Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPTP-MPPC-Compression</td>
<td></td>
<td>37</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>Primary-DNS</td>
<td>Y</td>
<td>5</td>
<td>String</td>
<td>Single</td>
<td>An IP address</td>
</tr>
<tr>
<td>Primary-WINS</td>
<td>Y</td>
<td>7</td>
<td>String</td>
<td>Single</td>
<td>An IP address</td>
</tr>
<tr>
<td>Privilege-Level</td>
<td>Y</td>
<td>220</td>
<td>Integer</td>
<td>Single</td>
<td>An integer between 0 and 15.</td>
</tr>
<tr>
<td>Required-Client- Firewall-Vendor-Code</td>
<td>Y</td>
<td>45</td>
<td>Integer</td>
<td>Single</td>
<td>1 = Cisco Systems (with Cisco Integrated Client) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (with Cisco Intrusion Prevention Security Agent)</td>
</tr>
<tr>
<td>Required-Client-Firewall-Description</td>
<td>Y</td>
<td>47</td>
<td>String</td>
<td>Single</td>
<td>String</td>
</tr>
<tr>
<td>Required-Client-Firewall-Product-Code</td>
<td>Y</td>
<td>46</td>
<td>Integer</td>
<td>Single</td>
<td>Cisco Systems Products: 1 = Cisco Intrusion Prevention Security Agent or Cisco Integrated Client (CIC) Zone Labs Products: 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE Product: 1 = BlackIce Defender/Agent Sygate Products: 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent</td>
</tr>
<tr>
<td>Required-Individual-User-Auth</td>
<td>Y</td>
<td>49</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>Require-HW-Client-Auth</td>
<td>Y</td>
<td>48</td>
<td>Boolean</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>Secondary-DNS</td>
<td>Y</td>
<td>6</td>
<td>String</td>
<td>Single</td>
<td>An IP address</td>
</tr>
<tr>
<td>Secondary-WINS</td>
<td>Y</td>
<td>8</td>
<td>String</td>
<td>Single</td>
<td>An IP address</td>
</tr>
<tr>
<td>SEP-Card-Assignment</td>
<td></td>
<td>9</td>
<td>Integer</td>
<td>Single</td>
<td>Not used</td>
</tr>
<tr>
<td>Session Subtype</td>
<td>Y</td>
<td>152</td>
<td>Integer</td>
<td>Single</td>
<td>0 = None 1 = Clientless 2 = Client 3 = Client Only Session Subtype applies only when the Session Type (151) attribute has the following values: 1, 2, 3, and 4.</td>
</tr>
</tbody>
</table>
### Table 29-1: Supported RADIUS Authorization Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Type</td>
<td>Y</td>
<td>151</td>
<td>Integer</td>
<td>Single</td>
<td>0 = None 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN (IKEv2) 3 = Clientless SSL VPN 4 = Clientless Email Proxy 5 = Cisco VPN Client (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN Load Balancing</td>
</tr>
<tr>
<td>Simultaneous-Logins</td>
<td>Y</td>
<td>2</td>
<td>Integer</td>
<td>Single</td>
<td>0-2147483647</td>
</tr>
<tr>
<td>Smart-Tunnel</td>
<td>Y</td>
<td>136</td>
<td>String</td>
<td>Single</td>
<td>Name of a Smart Tunnel</td>
</tr>
<tr>
<td>Smart-Tunnel-Auto</td>
<td>Y</td>
<td>138</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled 2 = AutoStart</td>
</tr>
<tr>
<td>Smart-Tunnel-Auto-Signon-Enable</td>
<td>Y</td>
<td>139</td>
<td>String</td>
<td>Single</td>
<td>Name of a Smart Tunnel Auto Signon list appended by the domain name</td>
</tr>
<tr>
<td>Strip-Realm</td>
<td>Y</td>
<td>135</td>
<td>Boolean</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>SVC-Ask</td>
<td>Y</td>
<td>131</td>
<td>String</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled 3 = Enable default service 5 = Enable default clientless (2 and 4 not used)</td>
</tr>
<tr>
<td>SVC-Ask-Timeout</td>
<td>Y</td>
<td>132</td>
<td>Integer</td>
<td>Single</td>
<td>5-120 seconds</td>
</tr>
<tr>
<td>SVC-DPD-Interval-Client</td>
<td>Y</td>
<td>108</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Off 5-3600 seconds</td>
</tr>
<tr>
<td>SVC-DPD-Interval-Gateway</td>
<td>Y</td>
<td>109</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Off) 5-3600 seconds</td>
</tr>
<tr>
<td>SVC-DTLS</td>
<td>Y</td>
<td>123</td>
<td>Integer</td>
<td>Single</td>
<td>0 = False 1 = True</td>
</tr>
<tr>
<td>SVC-Keepalive</td>
<td>Y</td>
<td>107</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Off 15-600 seconds</td>
</tr>
<tr>
<td>SVC-Modules</td>
<td>Y</td>
<td>127</td>
<td>String</td>
<td>Single</td>
<td>String (name of a module)</td>
</tr>
<tr>
<td>SVC-MTU</td>
<td>Y</td>
<td>125</td>
<td>Integer</td>
<td>Single</td>
<td>MTU value 256-1406 in bytes</td>
</tr>
<tr>
<td>SVC-Profiles</td>
<td>Y</td>
<td>128</td>
<td>String</td>
<td>Single</td>
<td>String (name of a profile)</td>
</tr>
<tr>
<td>SVC-Rekey-Time</td>
<td>Y</td>
<td>110</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1-10080 minutes</td>
</tr>
<tr>
<td>Tunnel Group Name</td>
<td>Y</td>
<td>146</td>
<td>String</td>
<td>Single</td>
<td>1-253 characters</td>
</tr>
<tr>
<td>Tunnel-Group-Lock</td>
<td>Y</td>
<td>85</td>
<td>String</td>
<td>Single</td>
<td>Name of the tunnel group or “none”</td>
</tr>
</tbody>
</table>
### Table 29-1  Supported RADIUS Authorization Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
</table>
| Tunneling-Protocols                                 | Y   | 11        | Integer     | Single                 | 1 = PPTP  
2 = L2TP  
4 = IPSec (IKEv1)  
8 = L2TP/IPSec  
16 = WebVPN  
32 = SVC  
64 = IPsec (IKEv2)  
8 and 4 are mutually exclusive.  
0 - 11, 16 - 27, 32 - 43, 48 - 59 are legal values. |
| Use-Client-Address                                 |     | 17        | Boolean     | Single                 | 0 = Disabled  
1 = Enabled                                                                                             |
| VLAN                                                | Y   | 140       | Integer     | Single                 | 0-4094                                                                                      |
| WebVPN-Access-List                                 | Y   | 73        | String      | Single                 | Access-List name                                                                       |
| WebVPN ACL                                          | Y   | 73        | String      | Single                 | Name of a WebVPN ACL on the device                                                      |
| WebVPN-ActiveX-Relay                                | Y   | 137       | Integer     | Single                 | 0 = Disabled  
Otherwise = Enabled                                                                                       |
| WebVPN-Apply-ACL                                    | Y   | 102       | Integer     | Single                 | 0 = Disabled  
1 = Enabled                                                                                             |
| WebVPN-Auto-HTTP-Signon                            | Y   | 124       | String      | Single                 | Reserved                                                                                   |
| WebVPN-Citrix-Metaframe-Enable                      | Y   | 101       | Integer     | Single                 | 0 = Disabled  
1 = Enabled                                                                                             |
| WebVPN-Content-Filter-Parameters                    | Y   | 69        | Integer     | Single                 | 1 = Java ActiveX  
2 = Java Script  
4 = Image  
8 = Cookies in images                                                                                   |
| WebVPN-Customization                               | Y   | 113       | String      | Single                 | Name of the customization                                                              |
| WebVPN-Default-Homepage                            | Y   | 76        | String      | Single                 | A URL such as http://example-example.com                                                  |
| WebVPN-Deny-Message                                | Y   | 116       | String      | Single                 | Valid string (up to 500 characters)                                                      |
| WebVPN-Download_Max-Size                           | Y   | 157       | Integer     | Single                 | 0x7fffffff                                                                                  |
| WebVPN-File-Access-Enable                          | Y   | 94        | Integer     | Single                 | 0 = Disabled  
1 = Enabled                                                                                             |
| WebVPN-File-Server-Browsing-Enable                 | Y   | 96        | Integer     | Single                 | 0 = Disabled  
1 = Enabled                                                                                             |
| WebVPN-File-Server-Entry-Enable                    | Y   | 95        | Integer     | Single                 | 0 = Disabled  
1 = Enabled                                                                                             |
### Table 29-1 Supported RADIUS Authorization Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebVPN-Hidden-Shares</td>
<td>Y</td>
<td>126</td>
<td>Integer</td>
<td>Single</td>
<td>0 = None 1 = Visible</td>
</tr>
<tr>
<td>WebVPN-Home-Page-Use-Smart-Tunnel</td>
<td>Y</td>
<td>228</td>
<td>Boolean</td>
<td>Single</td>
<td>Enabled if clientless home page is to be rendered through Smart Tunnel.</td>
</tr>
<tr>
<td>WebVPN-HTML-Filter</td>
<td>Y</td>
<td>69</td>
<td>Bitmap</td>
<td>Single</td>
<td>1 = Java ActiveX 2 = Scripts 4 = Image 8 = Cookies</td>
</tr>
<tr>
<td>WebVPN-HTTP-Compression</td>
<td>Y</td>
<td>120</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Off 1 = Deflate Compression</td>
</tr>
<tr>
<td>WebVPN-HTTP-Proxy-IP-Address</td>
<td>Y</td>
<td>74</td>
<td>String</td>
<td>Single</td>
<td>Comma-separated DNS/IP:port, with http= or https= prefix (for example http=10.10.10.10:80, https=11.11.11.11:443)</td>
</tr>
<tr>
<td>WebVPN-Idle-Timeout-Alert-Interval</td>
<td>Y</td>
<td>148</td>
<td>Integer</td>
<td>Single</td>
<td>0-30. 0 = Disabled.</td>
</tr>
<tr>
<td>WebVPN-Keepalive-Ignore</td>
<td>Y</td>
<td>121</td>
<td>Integer</td>
<td>Single</td>
<td>0-900</td>
</tr>
<tr>
<td>WebVPN-Macro-Substitution</td>
<td>Y</td>
<td>223</td>
<td>String</td>
<td>Single</td>
<td>Unbounded. For examples, see the SSL VPN Deployment Guide at the following URL: <a href="http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html</a></td>
</tr>
<tr>
<td>WebVPN-Macro-Substitution</td>
<td>Y</td>
<td>224</td>
<td>String</td>
<td>Single</td>
<td>Unbounded. For examples, see the SSL VPN Deployment Guide at the following URL: <a href="http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html</a></td>
</tr>
<tr>
<td>WebVPN-Port-Forwarding-Enable</td>
<td>Y</td>
<td>97</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-Port-Forwarding-Exchange-Proxy-Enable</td>
<td>Y</td>
<td>98</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-Port-Forwarding-HTTP-Proxy</td>
<td>Y</td>
<td>99</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-Port-Forwarding-List</td>
<td>Y</td>
<td>72</td>
<td>String</td>
<td>Single</td>
<td>Port forwarding list name</td>
</tr>
<tr>
<td>WebVPN-Port-Forwarding-Name</td>
<td>Y</td>
<td>79</td>
<td>String</td>
<td>Single</td>
<td>String name (example, “Corporate-Apps”). This text replaces the default string, “Application Access,” on the clientless portal home page.</td>
</tr>
<tr>
<td>WebVPN-Post-Max-Size</td>
<td>Y</td>
<td>159</td>
<td>Integer</td>
<td>Single</td>
<td>0x7fffffff</td>
</tr>
<tr>
<td>WebVPN-Session-Timeout-Alert-Interval</td>
<td>Y</td>
<td>149</td>
<td>Integer</td>
<td>Single</td>
<td>0-30. 0 = Disabled.</td>
</tr>
</tbody>
</table>
## Table 29-1  Supported RADIUS Authorization Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebVPN Smart-Card-Removal-Disconnect</td>
<td>Y</td>
<td>225</td>
<td>Boolean</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-Smart-Tunnel</td>
<td>Y</td>
<td>136</td>
<td>String</td>
<td>Single</td>
<td>Name of a Smart Tunnel</td>
</tr>
<tr>
<td>WebVPN-Smart-Tunnel-Auto-Sign-On</td>
<td>Y</td>
<td>139</td>
<td>String</td>
<td>Single</td>
<td>Name of a Smart Tunnel auto sign-on list appended by the domain name</td>
</tr>
<tr>
<td>WebVPN-Smart-Tunnel-Auto-Start</td>
<td>Y</td>
<td>138</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled 2 = Auto Start</td>
</tr>
<tr>
<td>WebVPN-Smart-Tunnel-Tunnel-Policy</td>
<td>Y</td>
<td>227</td>
<td>String</td>
<td>Single</td>
<td>One of “e networkname,” “i networkname,” or “a,” where networkname is the name of a Smart Tunnel network list, e indicates the tunnel excluded, i indicates the tunnel specified, and a indicates all tunnels.</td>
</tr>
<tr>
<td>WebVPN-SSL-VPN-Client-Enable</td>
<td>Y</td>
<td>103</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-SSL-VPN-Client-Keep-Installation</td>
<td>Y</td>
<td>105</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-SSL-VPN-Client-Required</td>
<td>Y</td>
<td>104</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-SSO-Server-Name</td>
<td>Y</td>
<td>114</td>
<td>String</td>
<td>Single</td>
<td>Valid string</td>
</tr>
<tr>
<td>WebVPN-Storage-Key</td>
<td>Y</td>
<td>162</td>
<td>String</td>
<td>Single</td>
<td></td>
</tr>
<tr>
<td>WebVPN-Storage-Objects</td>
<td>Y</td>
<td>161</td>
<td>String</td>
<td>Single</td>
<td></td>
</tr>
<tr>
<td>WebVPN-SVC-Keepalive-Frequency</td>
<td>Y</td>
<td>107</td>
<td>Integer</td>
<td>Single</td>
<td>15-600 seconds, 0=Off</td>
</tr>
<tr>
<td>WebVPN-SVC-Client-DPD-Frequency</td>
<td>Y</td>
<td>108</td>
<td>Integer</td>
<td>Single</td>
<td>5-3600 seconds, 0=Off</td>
</tr>
<tr>
<td>WebVPN-SVC-DTLS-Enable</td>
<td>Y</td>
<td>123</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-SVC-DTLS-MTU</td>
<td>Y</td>
<td>125</td>
<td>Integer</td>
<td>Single</td>
<td>MTU value is from 256-1406 bytes.</td>
</tr>
<tr>
<td>WebVPN-SVC-Gateway-DPD-Frequency</td>
<td>Y</td>
<td>109</td>
<td>Integer</td>
<td>Single</td>
<td>5-3600 seconds, 0=Off</td>
</tr>
<tr>
<td>WebVPN-SVC-Rekey-Time</td>
<td>Y</td>
<td>110</td>
<td>Integer</td>
<td>Single</td>
<td>4-10080 minutes, 0=Off</td>
</tr>
<tr>
<td>WebVPN-SVC-Rekey-Method</td>
<td>Y</td>
<td>111</td>
<td>Integer</td>
<td>Single</td>
<td>0 (Off), 1 (SSL), 2 (New Tunnel)</td>
</tr>
<tr>
<td>WebVPN-SVC-Compression</td>
<td>Y</td>
<td>112</td>
<td>Integer</td>
<td>Single</td>
<td>0 (Off), 1 (Deflate Compression)</td>
</tr>
<tr>
<td>WebVPN-UNIX-Group-ID (GID)</td>
<td>Y</td>
<td>222</td>
<td>Integer</td>
<td>Single</td>
<td>Valid UNIX group IDs</td>
</tr>
<tr>
<td>WebVPN-UNIX-User-ID (UIDs)</td>
<td>Y</td>
<td>221</td>
<td>Integer</td>
<td>Single</td>
<td>Valid UNIX user IDs</td>
</tr>
<tr>
<td>WebVPN-Upload-Max-Size</td>
<td>Y</td>
<td>158</td>
<td>Integer</td>
<td>Single</td>
<td>0xffffffff</td>
</tr>
<tr>
<td>WebVPN-URL-Entry-Enable</td>
<td>Y</td>
<td>93</td>
<td>Integer</td>
<td>Single</td>
<td>0 = Disabled 1 = Enabled</td>
</tr>
<tr>
<td>WebVPN-URL-List</td>
<td>Y</td>
<td>71</td>
<td>String</td>
<td>Single</td>
<td>URL list name</td>
</tr>
</tbody>
</table>
## About RADIUS Servers for AAA

### Supported IETF RADIUS Authorization Attributes

Table 29-2 lists the supported IETF RADIUS attributes.

### Table 29-2  Supported IETF RADIUS Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ASA</th>
<th>Attr. No.</th>
<th>Syntax/Type</th>
<th>Single or Multi-Valued</th>
<th>Description or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF-Radius-Class</td>
<td>Y</td>
<td>25</td>
<td>Single</td>
<td>25</td>
<td>For Versions 8.2.x and later, we recommend that you use the Group-Policy attribute (VSA 3076, #25) as described in Table 29-1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• group policy name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• OU=group policy name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• OU=group policy name</td>
</tr>
<tr>
<td>IETF-Radius-Filter-Id</td>
<td>Y</td>
<td>11</td>
<td>Single</td>
<td>11</td>
<td>ACL name that is defined on the ASA, which applies only to full tunnel IPsec and SSL VPN clients.</td>
</tr>
<tr>
<td>IETF-Radius-Framed-IP-Address</td>
<td>Y</td>
<td>6</td>
<td>String</td>
<td>6</td>
<td>An IP address</td>
</tr>
<tr>
<td>IETF-Radius-Framed-IP-Netmask</td>
<td>Y</td>
<td>28</td>
<td>Integer</td>
<td>28</td>
<td>An IP address mask</td>
</tr>
<tr>
<td>IETF-Radius-Idle-Timeout</td>
<td>Y</td>
<td>27</td>
<td>Integer</td>
<td>27</td>
<td>Seconds. Possible Service Type values:</td>
</tr>
<tr>
<td>IETF-Radius-Service-Type</td>
<td>Y</td>
<td>6</td>
<td>Integer</td>
<td>6</td>
<td>• .Administrative—User is allowed access to the configure prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• .NAS-Prompt—User is allowed access to the exec prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• .remote-access—User is allowed network access</td>
</tr>
<tr>
<td>IETF-Radius-Session-Timeout</td>
<td>Y</td>
<td>27</td>
<td>Integer</td>
<td>27</td>
<td>Seconds</td>
</tr>
</tbody>
</table>
RADIUS Accounting Disconnect Reason Codes

These codes are returned if the ASA encounters a disconnect when sending packets:

<table>
<thead>
<tr>
<th>Disconnect Reason Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCT_DISC_USER_REQ</td>
<td>1</td>
</tr>
<tr>
<td>ACCT_DISC_LOST_CARRIER</td>
<td>2</td>
</tr>
<tr>
<td>ACCT_DISC_LOST_SERVICE</td>
<td>3</td>
</tr>
<tr>
<td>ACCT_DISC_IDLE_TIMEOUT</td>
<td>4</td>
</tr>
<tr>
<td>ACCT_DISC_SESS_TIMEOUT</td>
<td>5</td>
</tr>
<tr>
<td>ACCT_DISC_ADMIN_RESET</td>
<td>6</td>
</tr>
<tr>
<td>ACCT_DISC_ADMIN_REBOOT</td>
<td>7</td>
</tr>
<tr>
<td>ACCT_DISC_PORT_ERROR</td>
<td>8</td>
</tr>
<tr>
<td>ACCT_DISC_NAS_ERROR</td>
<td>9</td>
</tr>
<tr>
<td>ACCT_DISC_NAS_REQUEST</td>
<td>10</td>
</tr>
<tr>
<td>ACCT_DISC_NAS_REBOOT</td>
<td>11</td>
</tr>
<tr>
<td>ACCT_DISC_PORT_UNNEEDED</td>
<td>12</td>
</tr>
<tr>
<td>ACCT_DISC_PORT_PREEMPTED</td>
<td>13</td>
</tr>
<tr>
<td>ACCT_DISC_PORT_SUSPENDED</td>
<td>14</td>
</tr>
<tr>
<td>ACCT_DISC_SERV_UNAVAIL</td>
<td>15</td>
</tr>
<tr>
<td>ACCT_DISC_CALLBACK</td>
<td>16</td>
</tr>
<tr>
<td>ACCT_DISC_USER_ERROR</td>
<td>17</td>
</tr>
<tr>
<td>ACCT_DISC_HOST_REQUEST</td>
<td>18</td>
</tr>
<tr>
<td>ACCT_DISC_ADMIN_SHUTDOWN</td>
<td>19</td>
</tr>
<tr>
<td>ACCT_DISC_SA_EXPIRED</td>
<td>21</td>
</tr>
<tr>
<td>ACCT_DISC_MAX_REASONS</td>
<td>22</td>
</tr>
</tbody>
</table>

Guidelines for RADIUS Servers for AAA

This section includes the guidelines and limitations that you should check before configuring RADIUS servers for AAA.

IPv6
The AAA server must use an IPv4 address, but endpoints can use IPv6.

Additional Guidelines
- You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 4 servers in multiple mode.

Related Topics
- Fallback Support, page 28-2
Configure RADIUS Servers for AAA

Configure RADIUS servers for AAA by performing the following tasks:

**Step 1** Load the ASA attributes into the RADIUS server. The method that you use to load the attributes depends on which type of RADIUS server that you are using:

- If you are using Cisco ACS: the server already has these attributes integrated. You can skip this step.
- For RADIUS servers from other vendors (for example, Microsoft Internet Authentication Service): you must manually define each ASA attribute. To define an attribute, use the attribute name or number, type, value, and vendor code (3076).

**Step 2** Add a RADIUS server group. See Configure RADIUS Server Groups, page 29-14.

**Step 3** For a server group, add a server to the group. See Add a RADIUS Server to a Group, page 29-17.

Configure RADIUS Server Groups

If you want to use an external RADIUS server for authentication, authorization, or accounting, you must first create at least one RADIUS server group per AAA protocol and add one or more servers to each group. You identify AAA server groups by name.

To add a RADIUS server group, perform the following steps:

**Procedure**

**Step 1** Identify the server group name and the protocol.

`aaa-server server_tag protocol radius`

Example:

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

When you enter the `aaa-server protocol` command, you enter aaa-server group configuration mode.

**Step 2** Merge a downloadable ACL with the ACL received in the Cisco AV pair from a RADIUS packet.

`merge-dacl {before-avpair | after-avpair}`

Example:

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

The default setting is `no merge dacl`, which specifies that downloadable ACLs will not be merged with Cisco AV pair ACLs. If both an AV pair and a downloadable ACL are received, the AV pair has priority and is used.

The `before-avpair` option specifies that the downloadable ACL entries should be placed before the Cisco AV pair entries.
The `after-avpair` option specifies that the downloadable ACL entries should be placed after the Cisco AV pair entries. This option applies only to VPN connections. For VPN users, ACLs can be in the form of Cisco AV pair ACLs, downloadable ACLs, and an ACL that is configured on the ASA. This option determines whether or not the downloadable ACL and the AV pair ACL are merged, and does not apply to any ACLs configured on the ASA.

**Step 3** Specify the maximum number of requests that can be sent to a RADIUS server in the group before the ASA tries the next server.

```
max-failed-attempts number
```

Example:

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

The `number` argument can range from 1 and 5. The default is 3.

If you configured a fallback method using the local database (for management access only), and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. If you do not have a fallback method, the ASA continues to retry the servers in the group.

**Step 4** Specify the method (reactivation policy) by which failed servers in a group are reactivated.

```
reactivation-mode {depletion [deadtime minutes] | timed}
```

Example:

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

The `depletion` keyword reactivates failed servers only after all of the servers in the group are inactive. The `deadtime minutes` keyword-argument pair specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes.

The `timed` keyword reactivates failed servers after 30 seconds of down time.

**Step 5** Send accounting messages to all servers in the group.

```
accounting-mode simultaneous
```

Example:

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Enter the `accounting-mode single` command to restore the default of sending messages only to the active server.

**Step 6** Identify the server and the AAA server group to which it belongs.

```
aaa-server server_group [interface_name] host server_ip
```

Example:

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

When you enter the `aaa-server host` command, you enter aaa-server host configuration mode.

**Step 7** Enable the RADIUS Dynamic Authorization (CoA) services for the AAA server group.

```
dynamic-authorization {port port-number}
```

Example:
Configure RADIUS Servers for AAA

Chapter 29      RADIUS + Servers for AAA

Step 8

Enable authorize-only mode for the RADIUS server group.

authorize-only

Example:

ciscoasa(config-aaa-server-group)# authorize-only

When this server group is used for authorization, the RADIUS Access Request message will be built as an “Authorize Only” request instead of the configured password methods that are available now.

The Authorize-Only request includes a Service-Type attribute with value Authorize-Only (17) and message authenticator within the Access-Request.

The support of the authorize-only mode eliminates the need of including the RADIUS common password in the Access-Request. Thus, it does not require the configuration of common password using the radius-common-pw CLI in the aaa-server-host mode.

Note

The authorize-only mode is configured for the server group; however, the common password is host-specific. Thus, once authorize-only mode is configured, the common password configured for an individual AAA server would be ignored.

Step 9

Switch off hostscan processing for connections that are made to a specific tunnel group.

without-csd (anyconnect)

Example:

ciscoasa(config-tunnel-webvpn)# without-csd anyconnect

This setting currently applies to clientless and Layer 3 connections. This command has been modified to allow this setting to be applied to AnyConnect connections only.

Examples

The following example shows how to add one RADIUS group with a single server:

ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit

The following example shows how to configure an ISE server object for authorization-only, dynamic authorization (CoA) updates, and hourly periodic accounting:

ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
Configure RADIUS Servers for AAA

The following example shows how to configure a tunnel group for password authentication with ISE:

```ciscoasa(config)# tunnel-group aaa-coa general-attributes
  ciscoasa(config-tunnel-general)# address-pool vpn
  ciscoasa(config-tunnel-general)# authentication-server-group ise
  ciscoasa(config-tunnel-general)# exit
```

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE:

```ciscoasa(config)# tunnel-group aaa-coa general-attributes
  ciscoasa(config-tunnel-general)# address-pool vpn
  ciscoasa(config-tunnel-general)# authentication certificate
  ciscoasa(config-tunnel-general)# authorization-server-group ise
  ciscoasa(config-tunnel-general)# accounting-server-group ise
  ciscoasa(config-tunnel-general)# exit
```

Add a RADIUS Server to a Group

To add a RADIUS server to a group, perform the following steps:

**Procedure**

**Step 1** Identify the RADIUS server and the AAA server group to which it belongs.

```ciscoasa(config)# aaa-server server_group [interface_name] host server_ip
```

Example:

```ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

When you enter the `aaa-server host` command, you enter aaa-server host configuration mode.

**Step 2** Specify how the ASA treats netmasks received in a downloadable ACL from a RADIUS server that is accessed by using the `aaa-server host` command.

```ciscoasa(config-aaa-server-host)# acl-netmask-convert {auto-detect | standard | wildcard}
```

Example:

```ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

The **auto-detect** keyword specifies that the ASA should attempt to determine the type of netmask expression used. If the ASA detects a wildcard netmask expression, it converts it to a standard netmask expression.

The **standard** keyword specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.

The **wildcard** keyword specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions and converts them all to standard netmask expressions when the ACLs are downloaded.
Step 3  Specify a common password to be used for all users who are accessing a RADIUS authorization server through the ASA.

```
radius-common-pw string
```

Example:

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

The `string` argument is a case-sensitive, alphanumeric keyword of up to 127 characters to be used as a common password for all authorization transactions with the RADIUS server.

Step 4  Enable MS-CHAPv2 authentication requests to the RADIUS server.

```
mschapv2-capable
```

Example:

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

Step 5  Specify the length of time, in seconds, that the ASA waits for a response from the primary server before sending the request to the backup server.

```
timeout hh:mm:ss
```

Example:

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Step 6  Configure the amount of time between retry attempts for a particular AAA server designated in a previous `aaa-server host` command.

```
retry-interval seconds
```

Example:

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

The `seconds` argument specifies the retry interval (1-10 seconds) for the request. This is the time that the ASA waits before retrying a connection request.

**Note**  The interval between subsequent retries will always be 50 or 100 milliseconds, regardless of the retry-interval settings you have entered. This is the intended behavior.

Step 7  Send accounting messages to all servers in the group.

```
accounting-mode simultaneous
```

Example:

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Enter the `accounting-mode single` command to restore the default of sending messages only to the active server.

Step 8  Specify the authentication port as port number1645, or the server port to be used for authentication of users.

```
authentication-port port
```

Example:

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```
Step 9 Specify the accounting port as port number 1646, or the server port to be used for accounting for this host.

```
accounting-port port
```

Example:
```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

Step 10 Specify the server secret value used to authenticate the RADIUS server to the ASA. The server secret that you configure should match the one configured on the RADIUS server. If you do not know the server secret value, ask the RADIUS server administrator. The maximum length is 64 characters.

```
key
```

Example:
```
ciscoasa(config-aaa-host)# key myexamplekey1
```

The server secret that you configure should match the one configured on the RADIUS server. If you do not know the server secret value, ask the RADIUS server administrator. The maximum length is 64 characters.

Examples

The following example shows how to add a RADIUS server to an existing RADIUS server group:

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
물리적으로 연결된 RADIUS 서버와의 인증을 위해
Cisco ASA Series General Operations CLI Configuration Guide

Monitoring RADIUS Servers for AAA

See the following commands for monitoring the status of RADIUS servers for AAA:

- **show aaa-server**
  
  This command shows the configured RADIUS server statistics.

- **show running-config aaa-server**
  
  This command shows the RADIUS server running configuration.

- **clear aaa-server statistics**
  
  This command clears the RADIUS server configuration.
### History for RADIUS Servers for AAA

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Servers for AAA</td>
<td>7.0(1)</td>
<td>Describes how to configure RADIUS servers for AAA. We introduced the following commands: <code>aaa-server protocol</code>, <code>max-failed-attempts</code>, <code>reactivation-mode</code>, <code>accounting-mode simultaneous</code>, <code>aaa-server host</code>, <code>show aaa-server</code>, <code>show running-config aaa-server</code>, <code>clear aaa-server statistics</code>, <code>authentication-port</code>, <code>accounting-port</code>, <code>retry-interval</code>, <code>acl-netmask-convert</code>, <code>clear configure aaa-server</code>, <code>merge-dacl</code>, <code>radius-common-pw</code>, <code>key</code>.</td>
</tr>
<tr>
<td>Key vendor-specific attributes (VSAs) sent in RADIUS access request and accounting request packets from the ASA</td>
<td>8.4(3)</td>
<td>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.</td>
</tr>
</tbody>
</table>
TACACS+ Servers for AAA

This chapter describes how to configure TACACS+ servers used in AAA.

- About TACACS+ Servers for AAA, page 30-1
- Guidelines for TACACS+ Servers for AAA, page 30-2
- Configure TACACS+ Servers, page 30-3
- Monitoring TACACS+ Servers for AAA, page 30-5
- History for TACACS+ Servers for AAA, page 30-6

About TACACS+ Servers for AAA

The ASA supports TACACS+ server authentication with the following protocols: ASCII, PAP, CHAP, and MS-CHAPv1.

TACACS+ Attributes

The Cisco ASA provides support for TACACS+ attributes. TACACS+ attributes separate the functions of authentication, authorization, and accounting. The protocol supports two types of attributes: mandatory and optional. Both the server and client must understand a mandatory attribute, and the mandatory attribute must be applied to the user. An optional attribute may or may not be understood or used.

Note

To use TACACS+ attributes, make sure that you have enabled AAA services on the NAS.

Table 30-1 lists supported TACACS+ authorization response attributes for cut-through-proxy connections. Table 30-2 lists supported TACACS+ accounting attributes.

Table 30-1  Supported TACACS+ Authorization Response Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>Identifies a locally configured ACL to be applied to the connection.</td>
</tr>
</tbody>
</table>
Guidelines for TACACS+ Servers for AAA

This section includes guidelines and limitations that you should check before configuring TACACS+ servers for AAA.

IPv6
The AAA server must use an IPv4 address, but endpoints can use IPv6.

Additional Guidelines
- You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode.

---

Table 30-1

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idletime</td>
<td>Indicates the amount of inactivity in minutes that is allowed before the authenticated user session is terminated.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the absolute amount of time in minutes that authentication credentials remain active before the authenticated user session is terminated.</td>
</tr>
</tbody>
</table>

Table 30-2

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes_in</td>
<td>Specifies the number of input bytes transferred during this connection (stop records only).</td>
</tr>
<tr>
<td>bytes_out</td>
<td>Specifies the number of output bytes transferred during this connection (stop records only).</td>
</tr>
<tr>
<td>cmd</td>
<td>Defines the command executed (command accounting only).</td>
</tr>
<tr>
<td>disc-cause</td>
<td>Indicates the numeric code that identifies the reason for disconnecting (stop records only).</td>
</tr>
<tr>
<td>elapsed_time</td>
<td>Defines the elapsed time in seconds for the connection (stop records only).</td>
</tr>
<tr>
<td>foreign_ip</td>
<td>Specifies the IP address of the client for tunnel connections. Defines the address on the lowest security interface for cut-through-proxy connections.</td>
</tr>
<tr>
<td>local_ip</td>
<td>Specifies the IP address that the client connected to for tunnel connections. Defines the address on the highest security interface for cut-through-proxy connections.</td>
</tr>
<tr>
<td>NAS port</td>
<td>Contains a session ID for the connection.</td>
</tr>
<tr>
<td>packs_in</td>
<td>Specifies the number of input packets transferred during this connection.</td>
</tr>
<tr>
<td>packs_out</td>
<td>Specifies the number of output packets transferred during this connection.</td>
</tr>
<tr>
<td>priv-level</td>
<td>Set to the user privilege level for command accounting requests or to 1 otherwise.</td>
</tr>
<tr>
<td>rem_iddr</td>
<td>Indicates the IP address of the client.</td>
</tr>
<tr>
<td>service</td>
<td>Specifies the service used. Always set to “shell” for command accounting only.</td>
</tr>
<tr>
<td>task_id</td>
<td>Specifies a unique task ID for the accounting transaction.</td>
</tr>
<tr>
<td>username</td>
<td>Indicates the name of the user.</td>
</tr>
</tbody>
</table>
Configure TACACS+ Servers

Configure TACACS+ servers by performing the following tasks:

**Step 1**  Add a TACACS+ server group. See Configure TACACS+ Server Groups, page 30-3.

**Step 2**  For a server group, add a server to the group. See Add a TACACS+ Server to a Group, page 30-4.

Configure TACACS+ Server Groups

If you want to use a TACACS+ server for authentication, authorization, or accounting, you must first create at least one TACACS+ server group and add one or more servers to each group. You identify TACACS+ server groups by name.

To add a TACACS+ server group, perform the following steps:

**Procedure**

**Step 1**  Identify the server group name and the protocol.

```
aaa-server server_tag protocol tacacs+
```

Example:

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

When you enter the `aaa-server protocol` command, you enter aaa-server group configuration mode.

**Step 2**  Specify the maximum number of requests sent to a AAA server in the group before trying the next server.

```
max-failed-attempts number
```

Example:

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

The `number` argument can range from 1 and 5. The default is 3.

If you configured a fallback method using the local database (for management access only), and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the `reactivation-mode` command in the next step.

If you do not have a fallback method, the ASA continues to retry the servers in the group.
Step 3  Specify the method (reactivation policy) by which failed servers in a group are reactivated.

```
reactivation-mode (depletion [deadtime minutes] | timed)
```

Example:
```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

The **depletion** keyword reactivates failed servers only after all of the servers in the group are inactive.
The **deadtime minutes** keyword-argument pair specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes.

The **timed** keyword reactivates failed servers after 30 seconds of down time.

Step 4  Send accounting messages to all servers in the group.

```
accounting-mode simultaneous
```

Example:
```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

To restore the default of sending messages only to the active server, enter the **accounting-mode single** command.

---

**Examples**

The following example shows how to add one TACACS+ group with one primary and one backup server:
```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
exit

ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
```

---

Add a TACACS+ Server to a Group

To add a TACACS+ server to a group, perform the following steps:

**Procedure**

Step 1  Identify the TACACS+ server and the server group to which it belongs.
```
aaa-server server_group [interface_name] host server_ip
```

Example:
```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

When you enter the **aaa-server host** command, you enter aaa-server host configuration mode.
Step 2 Specify the length of time, in seconds, that the ASA waits for a response from the primary server before sending the request to the backup server.

```
timeout hh:mm:ss
```

Example:

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Step 3 Specify the server port as port number 49, or the TCP port number used by the ASA to communicate with the TACACS+ server.

```
server-port port_number
```

Example:

```
ciscoasa(config-aaa-server-host)# server-port 49
```

Step 4 Specify the server secret value used to authenticate the NAS to the TACACS+ server.

```
key
```

Example:

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

This value is a case-sensitive, alphanumeric keyword of up to 127 characters, which is the same value as the key on the TACACS+ server. Any characters over 127 are ignored. The key is used between the client and the server to encrypt data between them and must be the same on both the client and server systems. The key cannot contain spaces, but other special characters are allowed.

---

**Monitoring TACACS+ Servers for AAA**

See the following commands for monitoring TACACS+ servers for AAA:

- **show aaa-server**
  
  This command shows the configured TACACS+ server statistics. Enter the `clear aaa-server statistics` command to clear the TACACS+ server statistics.

- **show running-config aaa-server**
  
  This command shows the TACACS+ server running configuration. Enter the `clear configure aaa-server` command to clear the TACACS+ server configuration.
## History for TACACS+ Servers for AAA

### Table 30-3  History for TACACS+ Servers for AAA

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+ Servers</td>
<td>7.0(1)</td>
<td>Describes how to configure TACACS+ servers for AAA. We introduced the following commands: aaa-server protocol, max-failed-attempts, reactivation-mode, accounting-mode simultaneous, aaa-server host, aaa authorization exec authentication-server, server-port, key, clear aaa-server statistics, clear configure aaa-server, show aaa-server, show running-config aaa-server, username, service-type, timeout.</td>
</tr>
</tbody>
</table>
LDAP Servers for AAA

This chapter describes how to configure LDAP servers used in AAA.
- About LDAP and the ASA, page 31-1
- Guidelines for LDAP Servers for AAA, page 31-4
- Configure LDAP Servers for AAA, page 31-5
- Monitoring LDAP Servers for AAA, page 31-10
- History for LDAP Servers for AAA, page 31-10

About LDAP and the ASA

The Cisco ASA is compatible with the most LDAPv3 directory servers, including:
- Microsoft Active Directory
- Novell
- OpenLDAP

By default, the ASA autodetects whether it is connected to Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP, or a generic LDAPv3 directory server. However, if autodetection fails to determine the LDAP server type, you can manually configure it.

How Authentication Works with LDAP

During authentication, the ASA acts as a client proxy to the LDAP server for the user, and authenticates to the LDAP server in either plain text or by using the SASL protocol. By default, the ASA passes authentication parameters, usually a username and password, to the LDAP server in plain text.

The ASA supports the following SASL mechanisms, listed in order of increasing strength:
- Digest-MD5—The ASA responds to the LDAP server with an MD5 value computed from the username and password.
- Kerberos—The ASA responds to the LDAP server by sending the username and realm using the GSSAPI Kerberos mechanism.
The ASA and LDAP server supports any combination of these SASL mechanisms. If you configure multiple mechanisms, the ASA retrieves the list of SASL mechanisms that are configured on the server, and sets the authentication mechanism to the strongest one configured on both the ASA and the server. For example, if both the LDAP server and the ASA support both mechanisms, the ASA selects Kerberos, the stronger of the two.

When user LDAP authentication has succeeded, the LDAP server returns the attributes for the authenticated user. For VPN authentication, these attributes generally include authorization data that is applied to the VPN session. In this case, using LDAP accomplishes authentication and authorization in a single step.

**Note**

For more information about LDAP, see RFCs 1777, 2251, and 2849.

### LDAP Hierarchy

Your LDAP configuration should reflect the logical hierarchy of your organization. For example, suppose an employee at your company, Example Corporation, is named Employee1. Employee1 works in the Engineering group. Your LDAP hierarchy could have one or many levels. You might decide to set up a single-level hierarchy in which Employee1 is considered a member of Example Corporation. Or you could set up a multi-level hierarchy in which Employee1 is considered to be a member of the department Engineering, which is a member of an organizational unit called People, which is itself a member of Example Corporation. See Figure 31-1 for an example of a multi-level hierarchy.

A multi-level hierarchy has more detail, but searches return results more quickly in a single-level hierarchy.

**Figure 31-1**  
*A Multi-Level LDAP Hierarchy*

The ASA lets you tailor the search within the LDAP hierarchy. You configure the following three fields on the ASA to define where in the LDAP hierarchy that your search begins, the extent, and the type of information you are looking for. Together, these fields limit the search of the hierarchy to only the part that includes the user permissions.
Chapter 31: LDAP Servers for AAA

About LDAP and the ASA

- LDAP Base DN defines where in the LDAP hierarchy that the server should begin searching for user information when it receives an authorization request from the ASA.
- Search Scope defines the extent of the search in the LDAP hierarchy. The search proceeds this many levels in the hierarchy below the LDAP Base DN. You can choose to have the server search only the level immediately below it, or it can search the entire subtree. A single level search is quicker, but a subtree search is more extensive.
- Naming Attribute(s) defines the RDN that uniquely identifies an entry in the LDAP server. Common naming attributes can include cn (Common Name), sAMAccountName, and userPrincipalName.

Figure 31-1 shows a sample LDAP hierarchy for Example Corporation. Given this hierarchy, you could define your search in different ways. Table 31-1 shows two sample search configurations.

In the first example configuration, when Employee1 establishes the IPsec tunnel with LDAP authorization required, the ASA sends a search request to the LDAP server, indicating it should search for Employee1 in the Engineering group. This search is quick.

In the second example configuration, the ASA sends a search request indicating that the server should search for Employee1 within Example Corporation. This search takes longer.

### Table 31-1  Example Search Configurations

<table>
<thead>
<tr>
<th>No.</th>
<th>LDAP Base DN</th>
<th>Search Scope</th>
<th>Naming Attribute</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>group=Engineering,ou=People,dc=ExampleCorporation,dc=com</td>
<td>One Level</td>
<td>cn=Employee1</td>
<td>Quicker search</td>
</tr>
<tr>
<td>2</td>
<td>dc=ExampleCorporation,dc=com</td>
<td>Subtree</td>
<td>cn=Employee1</td>
<td>Longer search</td>
</tr>
</tbody>
</table>

Bind to an LDAP Server

The ASA uses the login DN and login password to establish trust (bind) with an LDAP server. When performing a Microsoft Active Directory read-only operation (such as authentication, authorization, or group search), the ASA can bind using a login DN with fewer privileges. For example, the login DN can be a user whose AD “Member Of” designation is part of Domain Users. For VPN password management operations, the login DN needs elevated privileges, and must be part of the Account Operators AD group.

The following is an example of a login DN:

cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com

The ASA supports the following authentication methods:

- Simple LDAP authentication with an unencrypted password on port 389
- Secure LDAP (LDAP-S) on port 636
- Simple Authentication and Security Layer (SASL) MD5
- SASL Kerberos

The ASA does not support anonymous authentication.

Note

As an LDAP client, the ASA does not support the transmission of anonymous binds or requests.
LDAP Attribute Maps

The ASA can use an LDAP directory for authenticating users for:

- VPN remote access users
- Firewall network access/cut-through-proxy sessions
- Setting policy permissions (also called authorization attributes), such as ACLs, bookmark lists, DNS or WINS settings, and session timers.
- Setting the key attributes in a local group policy

The ASA uses LDAP attribute maps to translate native LDAP user attributes to Cisco ASA attributes. You can bind these attribute maps to LDAP servers or remove them. You can also show or clear attribute maps.

The LDAP attribute map does not support multi-valued attributes. For example, if a user is a member of several AD groups, and the LDAP attribute map matches more than one group, the value chosen is based on the alphabetization of the matched entries.

To use the attribute mapping features correctly, you need to understand LDAP attribute names and values, as well as the user-defined attribute names and values.

The names of frequently mapped LDAP attributes and the type of user-defined attributes that they would commonly be mapped to include the following:

- IETF-Radius-Class (Group_Policy in ASA version 8.2 and later)—Sets the group policy based on the directory department or user group (for example, Microsoft Active Directory memberOf) attribute value. The group policy attribute replaced the IETF-Radius-Class attribute with ASDM version 6.2/ASA version 8.2 or later.
- IETF-Radius-Filter-Id—Applies an access control list or ACL to VPN clients, IPsec, and SSL.
- IETF-Radius-Framed-IP-Address—Assigns a static IP address assigned to a VPN remote access client, IPsec, and SSL.
- Banner1—Displays a text banner when the VPN remote access user logs in.
- Tunneling-Protocols—Allows or denies the VPN remote access session based on the access type.

Note A single LDAP attribute map may contain one or many attributes. You can only map one LDAP attribute from a specific LDAP server.

Guidelines for LDAP Servers for AAA

This section includes guidelines and limitations that you should check before configuring LDAP servers for AAA.

IPv6

The AAA server must use an IPv4 address, but endpoints can use IPv6.

Additional Guidelines

- The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACL on the default password policy.
Configure LDAP Servers for AAA

Configure LDAP servers for AAA by performing the following tasks:

- **Step 1**: Configure LDAP attribute maps. See Configure LDAP Attribute Maps, page 31-5.
- **Step 2**: Add an LDAP server group. See Configure LDAP Server Groups, page 31-7.
- **Step 3**: (Optional) Configure authorization from an LDAP server that is separate and distinct from the authentication mechanism. See Configure Authorization with LDAP for VPN, page 31-9.

Configure LDAP Attribute Maps

To configure LDAP attribute maps, perform the following steps:

**Procedure**

- **Step 1**: Create an unpopulated LDAP attribute map table.
  
  \[ \text{ldap attribute-map } \text{map-name} \]
  
  Example:
  
  `ciscoasa(config)# ldap attribute-map att_map_1`

- **Step 2**: Map the user-defined attribute name department to the Cisco attribute.
  
  \[ \text{map-name } \text{user-attribute-name } \text{Cisco-attribute-name} \]
  
  Example:
  
  `ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class`
Step 3 Map the user-defined map value department to the user-defined attribute value and the Cisco attribute value.

```
map-value user-attribute-name Cisco-attribute-name
```

Example:
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1

Step 4 Identify the server and the AAA server group to which it belongs.

```
aaa-server server_group [interface_name] host server_ip
```

Example:
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4

Step 5 Bind the attribute map to the LDAP server.

```
ldap-attribute-map map-name
```

Example:
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1

Examples

The following example shows how to limit management sessions to the ASA based on an LDAP attribute called accessType. The accessType attribute may have one of these values:

- VPN
- admin
- helpdesk

The following example shows how each value is mapped to one of the valid IETF-Radius-Service-Type attributes that the ASA supports: remote-access (Service-Type 5) Outbound, admin (Service-Type 6) Administrative, and nas-prompt (Service-Type 7) NAS Prompt.

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
```

```
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
```

```
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
```

```
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7
```

```
ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
```

```
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
```

```
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
```

```
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

```
ciscoasa(config-aaa-server-host)# ldap-login-password test
```

```
ciscoasa(config-aaa-server-host)# ldap-login-dn
CN=Administrator,CN=Users,DC=cisco,DC=local
```

```
ciscoasa(config-aaa-server-host)# server-type auto-detect
```

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

The following example shows how to display the complete list of Cisco LDAP attribute names:

```
ciscoasa(config)# ldap attribute-map att_map_1
```

```
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?
```

ldap mode commands/options:
cisco-attribute-names:
Access-Hours
Configure LDAP Servers for AAA

This section describes how to configure LDAP server groups.

Before You Begin
You must add an attribute map before you may add an LDAP server to an LDAP server group.
To create and configure an LDAP server group, then add an LDAP server to that group, perform the following steps:

Procedure

Step 1  Identify the server group name and the protocol.

```
aaa-server server_tag protocol ldap
```

Example:

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

When you enter the `aaa-server protocol` command, you enter aaa-server group configuration mode.

Step 2  Specify the maximum number of requests sent to an LDAP server in the group before trying the next server.

```
max-failed-attempts number
```

Example:

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

The `number` argument can range from 1 and 5. The default is 3.
If you configured a fallback method using the local database (for management access only) to configure the fallback mechanism, and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the `reactivation-mode` command in the next step.
If you do not have a fallback method, the ASA continues to retry the servers in the group.

Step 3  Specify the method (reactivation policy) by which failed servers in a group are reactivated.

```
reactivation-mode {depletion [deadtime minutes] | timed}
```

Example:

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```
Configure LDAP Servers for AAA

Configure LDAP Servers for AAA

The depletion keyword reactivates failed servers only after all of the servers in the group are inactive. The deadline minutes keyword-argument pair specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes.

The timed keyword reactivates failed servers after 30 seconds of down time.

**Step 4** Identify the LDAP server and AAA server group to which it belongs.

```
aaa-server server_group [interface_name] host server_ip
```

Example:

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

When you enter the `aaa-server host` command, you enter aaa-server host configuration mode. As needed, use host configuration mode commands to further configure the AAA server.

Table 31-2 lists the available commands for LDAP servers, and whether or not a new LDAP server definition has a default value for that command. If no default value is provided (indicated by “—”), use the command to specify the value.

<table>
<thead>
<tr>
<th>Command</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap-attribute-map</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ldap-base-dn</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ldap-login-dn</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ldap-login-password</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ldap-naming-attribute</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ldap-over-ssl</td>
<td>636</td>
<td>If not set, the ASA uses sAMAccountName for LDAP requests. Whether using SASL or plain text, you can secure communications between the ASA and the LDAP server with SSL. If you do not configure SASL, we strongly recommend that you secure LDAP communications with SSL.</td>
</tr>
<tr>
<td>ldap-scope</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>sasl-mechanism</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>server-port</td>
<td>389</td>
<td>—</td>
</tr>
<tr>
<td>server-type</td>
<td>autodiscovery</td>
<td>If autodetection fails to determine the LDAP server type, and you know the server is either a Microsoft, Sun or generic LDAP server, you can manually configure the server type.</td>
</tr>
<tr>
<td>timeout</td>
<td>10 seconds</td>
<td>—</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an LDAP server group named watchdogs and add an LDAP server to the group. Because the example does not define a retry interval or the port that the LDAP server listens to, the ASA uses the default values for these two server-specific parameters.

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
```
Configure Authorization with LDAP for VPN

When LDAP user authentication for VPN access has succeeded, the ASA queries the LDAP server, which returns LDAP attributes. These attributes generally include authorization data that applies to the VPN session. Using LDAP in this way accomplishes authentication and authorization in a single step. There may be cases, however, where you require authorization from an LDAP directory server that is separate and distinct from the authentication mechanism. For example, if you use an SDI or certificate server for authentication, no authorization information is returned. For user authorizations in this case, you can query an LDAP directory after successful authentication, accomplishing authentication and authorization in two steps.

To set up VPN user authorization using LDAP, perform the following steps.

**Procedure**

**Step 1** Create an IPsec remote access tunnel group named remotegrp.

```
tunnel-group groupname
```

Example:

```
ciscoasa(config)# tunnel-group remotegrp
```

**Step 2** Associate the server group and the tunnel group.

```
tunnel-group groupname general-attributes
```

Example:

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

**Step 3** Assign a new tunnel group to a previously created AAA server group for authorization.

```
authorization-server-group group-tag
```

Example:

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

**Examples**

While there are other authorization-related commands and options available for specific requirements, the following example shows commands for enabling user authorization with LDAP. The example then creates an IPsec remote access tunnel group named remote-1, and assigns that new tunnel group to the previously created ldap_dir_1 AAA server group for authorization:

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

After you complete this configuration work, you can then configure additional LDAP authorization parameters such as a directory password, a starting point for searching a directory, and the scope of a directory search by entering the following commands:
Monitoring LDAP Servers for AAA

See the following commands for monitoring LDAP servers for AAA:

- **show aaa-server**
  This command shows the configured AAA server statistics. Use the `clear aaa-server statistics` command to clear the AAA server configuration.

- **show running-config aaa-server**
  This command shows the AAA server running configuration. Use the `clear configure aaa-server` command to clear AAA server statistics.

History for LDAP Servers for AAA

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Servers for AAA</td>
<td>7.0(1)</td>
<td>LDAP Servers describe support for AAA and how to configure LDAP servers. We introduced the following commands: `username, aaa authorization exec authentication-server, aaa authentication console LOCAL, aaa authorization exec LOCAL, service-type, ldap attribute-map, aaa-server protocol, aaa authentication {telnet</td>
</tr>
</tbody>
</table>
Identity Firewall

This chapter describes how to configure the ASA for the Identity Firewall.

- About the Identity Firewall, page 32-1
- Guidelines for the Identity Firewall, page 32-7
- Prerequisites for the Identity Firewall, page 32-9
- Configure the Identity Firewall, page 32-10
- Examples for the Identity Firewall, page 32-19
- History for the Identity Firewall, page 32-22

About the Identity Firewall

In an enterprise, users often need access to one or more server resources. Typically, a firewall is not aware of the users’ identities and, therefore, cannot apply security policies based on identity. To configure per-user access policies, you must configure a user authentication proxy, which requires user interaction (a username/password query).

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 user names and user group names 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.

The Identity Firewall integrates with Microsoft 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 and allows transparent authentication for Active Directory users.

Identity-based firewall services enhance the existing access control and security policy mechanisms by allowing users or groups to be specified in place of source IP addresses. Identity-based security policies can be interleaved without restriction between traditional IP address-based rules.

The key benefits of the Identity Firewall include:

- Decoupling network topology from security policies
- Simplifying the creation of security policies
- Providing the ability to easily identify user activities on network resources
- Simplifying user activity monitoring
Architecture for Identity Firewall Deployments

The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping.

The identity firewall consists of three components:

- **ASA**
- **Microsoft Active Directory**
  Although Active Directory is part of the Identity Firewall on the ASA, Active Directory administrators manage it. The reliability and accuracy of the data depends on data in Active Directory.
- **Active Directory (AD) Agent**

*Note*  Windows 2003 R2 is not supported for the AD Agent server.

*Figure 32-1* show the components of the Identity Firewall. The succeeding table describes the roles of these components and how they communicate with one another.
### Features of the Identity Firewall

The Identity Firewall includes the following key features.

**Flexibility**

- The ASA can retrieve user identity and IP address mapping from the AD Agent by querying the AD Agent for each new IP address or by maintaining a local copy of the entire user identity and IP address database.
- Supports host group, subnet, or IP address for the destination of a user identity policy.

### About the Identity Firewall

The Identity Firewall includes the following key features.

- **Flexibility**
  - The ASA can retrieve user identity and IP address mapping from the AD Agent by querying the AD Agent for each new IP address or by maintaining a local copy of the entire user identity and IP address database.
  - Supports host group, subnet, or IP address for the destination of a user identity policy.

### Figure 32-1  Identity Firewall Components

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>On the ASA</strong>: Administrators configure local user groups and Identity Firewall policies.</td>
</tr>
<tr>
<td>2</td>
<td><strong>ASA &lt;-&gt; AD Server</strong>: The ASA sends an LDAP query for the Active Directory groups configured on the AD Server. The ASA consolidates local and Active Directory groups and applies access rules and Modular Policy Framework security policies based on user identity.</td>
</tr>
<tr>
<td>3</td>
<td><strong>ASA &lt;-&gt; AD Agent</strong>: Depending on the Identity Firewall configuration, the ASA downloads the IP-user database or sends a RADIUS request to the AD Agent that asks for the user’s IP address. The ASA forwards the new mapped entries that have been learned from web authentication and VPN sessions to the AD Agent.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Client &lt;-&gt; ASA</strong>: The client logs into the network through Microsoft Active Directory. The AD Server authenticates users and generates user login security logs. Alternatively, the client can log into the network through a cut-through proxy or VPN.</td>
</tr>
<tr>
<td>5</td>
<td><strong>ASA &lt;-&gt; Client</strong>: Based on the policies configured on the ASA, it grants or denies access to the client. If configured, the ASA probes the NetBIOS of the client to pass inactive and no-response users.</td>
</tr>
<tr>
<td>6</td>
<td><strong>AD Agent &lt;-&gt; AD Server</strong>: The AD Agent maintains a cache of user ID and IP address mapped entries, and notifies the ASA of changes. The AD Agent sends logs to a syslog server.</td>
</tr>
</tbody>
</table>
• Supports a fully qualified domain name (FQDN) for the source and destination of a user identity policy.
• Supports the combination of 5-tuple policies with ID-based policies. The identity-based feature works in tandem with the existing 5-tuple solution.
• Supports use with IPS and Application Inspection policies.
• Retrieves user identity information from remote access VPN, AnyConnect VPN, L2TP VPN and cut-through proxy. All retrieved users are populated to all ASAs that are connected to the AD Agent.

**Scalability**

• Each AD Agent supports 100 ASAs. Multiple ASAs are able to communicate with a single AD Agent to provide scalability in larger network deployments.
• Supports 30 Active Directory servers provided the IP address is unique among all domains.
• Each user identity in a domain can have up to 8 IP addresses.
• Supports up to 64,000 user identity-IP address mapped entries in active policies for the ASA 5500 Series models. This limit controls the maximum number of users who have policies applied. The total number of users are the aggregate of all users configured in all different contexts.
• Supports up to 512 user groups in active ASA policies.
• A single access rule can contain one or more user groups or users.
• Supports multiple domains.

**Availability**

• The ASA retrieves group information from the Active Directory and falls back to web authentication for IP addresses when the AD Agent cannot map a source IP address to a user identity.
• The AD Agent continues to function when any of the Active Directory servers or the ASA are not responding.
• Supports configuring a primary AD Agent and a secondary AD Agent on the ASA. If the primary AD Agent stops responding, the ASA can switch to the secondary AD Agent.
• If the AD Agent is unavailable, the ASA can fall back to existing identity sources such as cut-through proxy and VPN authentication.
• The AD Agent runs a watchdog process that automatically restarts its services when they are down.
• Allows a distributed IP address/user mapping database for use among ASAs.

**Deployment Scenarios**

You can deploy the components of the Identity Firewall in the following ways, depending on your environmental requirements.

Figure 32-2 shows how you can deploy the components of the Identity Firewall to allow for redundancy. Scenario 1 shows a simple installation without component redundancy. Scenario 2 also shows a simple installation without redundancy. However, in this deployment scenario, the Active Directory server and AD Agent are co-located on the same Windows server.
Figure 32-2  Deployment Scenario without Redundancy

Scenario 1
AD Agent

Scenario 2
AD Server
AD Agent

AD Server
ASA

Figure 32-3 shows how you can deploy the Identity Firewall components to support redundancy. Scenario 1 shows a deployment with multiple Active Directory servers and a single AD Agent installed on a separate Windows server. Scenario 2 shows a deployment with multiple Active Directory servers and multiple AD Agents installed on separate Windows servers.

Figure 32-3  Deployment Scenario with Redundant Components

Scenario 1
AD Server
AD Agent

Scenario 2
AD Server
AD Agent

AD Server
ASA

AD Server
ASA

Figure 32-4 shows how all Identity Firewall components—Active Directory server, the AD Agent, and the clients—are installed and communicate on the LAN.
Figure 32-4  LAN-based Deployment

Figure 32-5 shows a WAN-based deployment to support a remote site. The Active Directory server and the AD Agent are installed on the main site LAN. The clients are located at a remote site and connect to the Identity Firewall components over a WAN.

Figure 32-5  WAN-based Deployment

Figure 32-6 also shows a WAN-based deployment to support a remote site. The Active Directory server is installed on the main site LAN. However, the AD Agent is installed and accessed by the clients at the remote site. The remote clients connect to the Active Directory servers at the main site over a WAN.
Figure 32-6  WAN-based Deployment with Remote AD Agent

Figure 32-7 shows an expanded remote site installation. An AD Agent and Active Directory servers are installed at the remote site. The clients access these components locally when logging into network resources located at the main site. The remote Active Directory server must synchronize its data with the central Active Directory servers located at the main site.

Figure 32-7  WAN-based Deployment with Remote AD Agent and AD Servers

Guidelines for the Identity Firewall

This section includes guidelines and limitations that you should check before configuring the Identity Firewall.

Failover

- The Identity Firewall supports user identity-IP address mapping and AD Agent status replication from active to standby when Stateful Failover is enabled. However, only user identity-IP address mapping, AD Agent status, and domain status are replicated. User and user group records are not replicated to the standby ASA.

- When failover is configured, the standby ASA must also be configured to connect to the AD Agent directly to retrieve user groups. The standby ASA does not send NetBIOS packets to clients even when the NetBIOS probing options are configured for the Identity Firewall.
• When a client is determined to be inactive by the active ASA, the information is propagated to the standby ASA. User statistics are not propagated to the standby ASA.

• When you have failover configured, you must configure the AD Agent to communicate with both the active and standby ASAs. See the *Installation and Setup Guide for the Active Directory Agent* for the steps to configure the ASA on the AD Agent server.

### IPv6

• The AD Agent supports endpoints with IPv6 addresses. It can receive IPv6 addresses in log events, maintain them in its cache, and send them through RADIUS messages. The AAA server must use an IPv4 address.

• NetBIOS over IPv6 is not supported.

### Additional Guidelines

• A full URL as a destination address is not supported.

• For NetBIOS probing to function, the network between the ASA, AD Agent, and clients must support UDP-encapsulated NetBIOS traffic.

• MAC address checking by the Identity Firewall does not work when intervening routers are present. Users logged into clients that are behind the same router have the same MAC addresses. With this implementation, all the packets from the same router are able to pass the check, because the ASA is unable to ascertain the actual MAC addresses behind the router.

• The following ASA features do not support using the identity-based object and FQDN in an extended ACL:
  - Route maps
  - Crypto maps
  - WCCP
  - NAT
  - Group policy (except for VPN filters)
  - DAP

• You can use the `user-identity update active-user-database` command to actively initiate a user-IP address download from the AD agent.

By design, if a previous download session has finished, the ASA does not allow you to issue this command again.

As a result, if the user-IP database is very large, the previous download session is not finished yet, and you issue another `user-identity update active-user-database` command, the following error message appears:

"ERROR: one update active-user-database is already in progress."

You need to wait until the previous session is completely finished, then you can issue another `user-identity update active-user-database` command.

Another example of this behavior occurs because of packet loss from the AD Agent to the ASA.

When you issue a `user-identity update active-user-database` command, the ASA requests the total number of user-IP mapped entries to be downloaded. Then the AD Agent initiates a UDP connection to the ASA and sends the change of authorization request packet.
If for some reason the packet is lost, there is no way for the ASA to discern this. As a result, the ASA holds the session for 4-5 minutes, during which time this error message continues to appear if you have issued the `user-identity update active-user-database` command.

- When you use the Cisco Context Directory Agent (CDA) in conjunction with the ASA or Cisco Ironport Web Security Appliance (WSA), make sure that you open the following ports:
  - Authentication port for UDP—1645
  - Accounting port for UDP—1646
  - Listening port for UDP—3799
  The listening port is used to send change of authorization requests from the CDA to the ASA or to the WSA.

- If the `user-identity action domain-controller-down domain_name disable-user-identity-rule` command is configured and the specified domain is down, or if the `user-identity action ad-agent-down disable-user-identity-rule` command is configured and the AD Agent is down, all the logged-in users have the disabled status.

- For domain names, the following characters are not valid: `\/:*?”<>|`. For naming conventions, see [http://support.microsoft.com/kb/909264](http://support.microsoft.com/kb/909264).

- For usernames, the following characters are not valid: `\/:*?”<>@`

- For user group names, the following characters are not valid: `\/:*?”<>`

- How you configure the Identity Firewall to retrieve user information from the AD Agent affects the amount of memory used by the feature. You specify whether the ASA uses on-demand retrieval or full download retrieval. Choosing on-demand retrieval has the benefit of using less memory, because only users of received packets are queried and stored.

## Prerequisites for the Identity Firewall

This section includes prerequisites for configuring the Identity Firewall.

**AD Agent**

- The AD Agent must be installed on a Windows server that is accessible to the ASA. Additionally, you must configure the AD Agent to obtain information from the Active Directory servers and to communicate with the ASA.


  **Note**
  Windows 2003 R2 is not supported for the AD Agent server.

- For the steps to install and configure the AD Agent, see the *Installation and Setup Guide for the Active Directory Agent*.

- Before configuring the AD Agent in the ASA, obtain the secret key value that the AD Agent and the ASA use to communicate. This value must match on both the AD Agent and the ASA.

**Microsoft Active Directory**

- Microsoft Active Directory must be installed on a Windows server and accessible by the ASA. Supported versions include Windows 2003, 2008, and 2008 R2 servers.
• Before configuring the Active Directory server on the ASA, create a user account in Active Directory for the ASA.

• Additionally, the ASA sends encrypted log-in information to the Active Directory server by using SSL enabled over LDAP. SSL must be enabled on the Active Directory server. See the documentation for Microsoft Active Directory for how to enable SSL for Active Directory.

---

**Note**

Before running the AD Agent Installer, you must install the patches listed in the *README First for the Cisco Active Directory Agent* on each Microsoft Active Directory server that the AD Agent monitors. These patches are required even when the AD Agent is installed directly on the domain controller server.

---

**Configure the Identity Firewall**

To configure the Identity Firewall, perform the following tasks:

---

**Step 1**

Configure the Active Directory domain in the ASA.

See *Configure the Active Directory Domain*, page 32-10.

See also *Deployment Scenarios*, page 32-4 for the ways in which you can deploy the Active Directory servers to meet your environment requirements.

**Step 2**

Configure the AD Agent in ASA.


See also *Deployment Scenarios*, page 32-4 for the ways in which you can deploy the AD Agents to meet your environment requirements.

**Step 3**

Configure Identity Options.

See *Configure Identity Options*, page 32-14.

**Step 4**

Configure Identity-based Security Policy. After the AD domain and AD Agent are configured, you can create identity-based object groups and ACLs for use in many features.


---

**Configure the Active Directory Domain**

Active Directory domain configuration on the ASA is required for the ASA to download Active Directory groups and accept user identities from specific domains when receiving IP-user mapping from the AD Agent.

**Before You Begin**

- Active Directory server IP address
- Distinguished Name for LDAP base DN
- Distinguished Name and password for the Active Directory user that the Identity Firewall uses to connect to the Active Directory domain controller
To configure the Active Directory domain, perform the following steps:

**Procedure**

**Step 1**
Create the AAA server group and configure AAA server parameters for the Active Directory server.

```
aaa-server server-tag protocol ldap
```

Example:
```
ciscoasa(config)# aaa-server adserver protocol ldap
```

**Step 2**
Configure the AAA server as part of a AAA server group and the AAA server parameters that are host-specific for the Active Directory server.

```
aaa-server server-tag [(interface-name)] host (server-ip | name) [key] [timeout seconds]
```

Example:
```
ciscoasa(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6
```

**Step 3**
Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.

```
ldap-base-dn string
```

Example:
```
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com
```

Specifying the `ldap-base-dn` command is optional. If you do not specify this command, the ASA retrieves the defaultNamingContext from the Active Directory and uses it as the base DN.

**Step 4**
Specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

```
ldap-scope subtree
```

Example:
```
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

**Step 5**
Specify the login password for the LDAP server.

```
ldap-login-password string
```

Example:
```
ciscoasa(config-aaa-server-host)# ldap-login-password obscurepassword
```

**Step 6**
Specify the name of the directory object that the system should bind this as.

```
ldap-login-dn string
```

Example:
```
ciscoasa(config-aaa-server-host)# ldap-login-dn SAMPLE\user1
```

The ASA identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field describes the authentication characteristics of the ASA. The `string` argument is a case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.
Configure the Identity Firewall

You can specify the traditional or simplified format. The typical `ldap-login-dn` command format includes: `CN=username,OU=Employees,OU=Sample Users,DC=sample,DC=com.`

**Step 7** Configure the LDAP server model for the Microsoft Active Directory server.

```bash
server-type microsoft
```

Example:

```
ciscoasa(config-aaa-server-host)# server-type microsoft
```

**Step 8** Specify the location of the Active Directory groups configuration in the Active Directory domain controller.

```bash
ldap-group-base-dn string
```

Example:

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com
```

If not specified, the value in the `ldap-group-base-dn` command is used. Specifying this command is optional.

**Step 9** Allow the ASA to access the Active Directory domain controller over SSL.

```bash
ldap-over-ssl enable
```

Example:

```
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
```

To support LDAP over SSL, Active Directory server needs to be configured to have this support. By default, the Active Directory does not have SSL configured. If SSL is not configured in the Active Directory, you do not need to configure it on the ASA for the Identity Firewall.

**Step 10** Specify the server port.

```bash
server-port port-number
```

Example:

```
ciscoasa(config-aaa-server-host)# server-port 389
ciscoasa(config-aaa-server-host)# server-port 636
```

By default, if the `ldap-over-ssl` command is not enabled, the default server port is 389; if the `ldap-over-ssl` command is enabled, the default server port is 636.

**Step 11** Set the amount of time before LDAP queries time out.

```bash
group-search-timeout seconds
```

Example:

```
ciscoasa(config-aaa-server-host)# group-search-timeout 300
```
Configure the Identity Firewall

Configure Active Directory Agents

Configure the primary and secondary AD Agents for the AD Agent Server Group. When the ASA detects that the primary AD Agent is not responding and a secondary agent is specified, the ASA switches to the secondary AD Agent. The Active Directory server for the AD agent uses RADIUS as the communication protocol; therefore, you should specify a key attribute for the shared secret between the ASA and AD Agent.

Before You Begin
- AD agent IP address
- Shared secret between the ASA and AD agent

To configure the AD Agents, perform the following steps:

Procedure

**Step 1** Create the AAA server group and configure AAA server parameters for the AD Agent.
```
aaa-server server-tag protocol radius
```
Example:
```
ciscoasa(config)# aaa-server adagent protocol radius
```

**Step 2** Enable the AD Agent mode.
```
ad-agent-mode
```
Example:
```
ciscoasa(config)# ad-agent-mode
```

**Step 3** Configure the AAA server as part of a AAA server group and the AAA server parameters that are host-specific for the AD Agent.
```
aaa-server server-tag [(interface-name)] host {server-ip | name} [key] [timeout seconds]
```
Example:
```
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
```

**Step 4** Specify the server secret value used to authenticate the ASA to the AD Agent server.
```
key key
```
Example:
```
ciscoasa(config-aaa-server-host)# key mysecret
```

**Step 5** Define the server group of the AD Agent.
```
user-identity ad-agent aaa-server aaa_server_group_tag
```
Example:
```
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
```

The first server defined in the `aaa_server_group_tag` argument is the primary AD Agent and the second server defined is the secondary AD Agent. The Identity Firewall supports defining only two AD Agent hosts.
When the ASA detects that the primary AD Agent is down and a secondary agent is specified, it switches to the secondary AD Agent. The AAA server for the AD agent uses RADIUS as the communication protocol, and should specify a key attribute for the shared secret between the ASA and AD Agent.

**Step 6** Test the communication between the ASA and the AD Agent server.

```plaintext
test aaa-server ad-agent
```

Example:

```
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

---

### Configure Identity Options

To configure the Identity Options for the Identity Firewall, perform the following steps:

**Procedure**

**Step 1** Enable the Identity Firewall feature. By default, the Identity Firewall feature is disabled.

```plaintext
user-identity enable
```

Example:

```
ciscoasa(config)# user-identity enable
```

**Step 2** Specify the default domain for the Identity Firewall.

```plaintext
user-identity default-domain domain_NetBIOS_name
```

Example:

```
ciscoasa(config)# user-identity default-domain SAMPLE
```

For the `domain_NetBIOS_name` argument, enter a name of up to 32 characters that consists of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,. ] except ‘.’ and ‘ ’ at the first character. If the domain name includes a space, enclose the entire name in quotation marks. The domain name is not case sensitive.

The default domain is used for all users and user groups when a domain has not been explicitly configured for those users or groups. When a default domain is not specified, the default domain for users and groups is LOCAL. For multiple context modes, you can set a default domain name for each context, as well as within the system execution space.

**Note** The default domain name that you specify must match the NetBIOS domain name configured on the Active Directory domain controller. If the domain name does not match, the AD Agent incorrectly associates the user identity-IP address mapped entries with the domain name that you enter when configuring the ASA. To view the NetBIOS domain name, open the Active Directory user event security log in any text editor.

The Identity Firewall uses the LOCAL domain for all locally defined user groups or locally defined users. Users logging in through a web portal (cut-through proxy) are designated as belonging to the Active Directory domain with which they authenticated. Users logging in through a VPN are designated as belonging to the LOCAL domain unless the VPN is authenticated by LDAP with the Active Directory. In this case, the Identity Firewall can associate the users with their Active Directory domain.
Step 3
Associate the LDAP parameters defined for the AAA server for importing user group queries with the domain name.

```
user-identity domain domainNickname aaa-server aaa_server_group_tag
```

Example:
```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

For the `domainNickname` argument, enter a name of up to 32 characters consisting of [a-z], [A-Z], [0-9], [@#$%^&()_-=+[]{};,. ] except `'` and `'` at the first character. If the domain name includes a space, you must enclose that space character in quotation marks. The domain name is not case sensitive.

Step 4
Enable NetBIOS probing.

```
user-identity logout-probe netbios local-system probe-time minutes retry-interval seconds retry-count times [user-not-needed | match-any | exact-match]
```

Example:
```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10 retry-interval seconds 10 retry-count 2 user-not-needed
```

Enabling this option configures how often the ASA probes the user client IP address to determine whether the client is still active. By default, NetBIOS probing is disabled. To minimize the NetBIOS packets, the ASA only sends a NetBIOS probe to a client when the user has been idle for more than the specified number of minutes.

- **Exact-match**—The username of the user assigned to the IP address must be the only one in the NetBIOS response. Otherwise, the user identity of that IP address is considered invalid.
- **User-not-needed**—As long as the ASA received a NetBIOS response from the client, the user identity is considered valid.

The Identity Firewall only performs NetBIOS probing for those users identities that are in the active state and exist in at least one security policy. The ASA does not perform NetBIOS probing for clients where the users logged in through cut-through proxy or by using a VPN.

Step 5
Specify the amount of time before a user is considered idle, meaning the ASA has not received traffic from the user's IP address for the specified amount of time.

```
user-identity inactive-user-timer minutes
```

Example:
```
ciscoasa(config)# user-identity inactive-user-timer minutes 120
```

When the timer expires, the user's IP address is marked as inactive and removed from the local cached user identity-IP address mapping database, and the ASA no longer notifies the AD Agent about that IP address. Existing traffic is still allowed to pass. When this command is specified, the ASA runs an inactive timer even when the NetBIOS Logout Probe is configured.

By default, the idle timeout is set to 60 minutes. This option does not apply to VPN or cut-through proxy users.

Step 6
Specify the amount of time before the ASA queries the Active Directory server for user group information.

```
user-identity poll-import-user-group-timer hours
```

Example:
```
ciscoasa(config)# user-identity poll-import-user-group-timer hours 1
```
If a user is added to or deleted from an Active Directory group, the ASA received the updated user group after the import group timer ran. By default, the **poll-import-user-group-timer hours** value is 8 hours. To immediately update user group information, enter the **user-identity update import-user** command.

**Step 7** Specify the action when a client does not respond to a NetBIOS probe.

```
user-identity action netbios-response-fail remove-user-ip
```

Example:
```
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip
```

For example, the network connection might be blocked to that client or the client is not active. When this command is configured, the ASA removes the user identity-IP address mapping for that client. By default, this command is disabled.

**Step 8** Specify the action when the domain is down, because the Active Directory domain controller is not responding.

```
user-identity action domain-controller-down domain_nickname disable-user-identity-rule
```

Example:
```
ciscoasa(config)# user-identity action domain-controller-down SAMPLE disable-user-identity-rule
```

When the domain is down and the **disable-user-identity-rule** keyword is configured, the ASA disables the user identity-IP address mapping for that domain. Additionally, the status of all user IP addresses in that domain are marked as disabled in the output displayed by the **show user-identity user** command. By default, this command is disabled.

**Step 9** Enable user-not-found tracking. By default, this command is disabled.

```
user-identity user-not-found enable
```

Example:
```
ciscoasa(config)# user-identity user-not-found enable
```

Only the last 1024 IP addresses are tracked.

**Step 10** Specify the action when the AD Agent is not responding.

```
user-identity action ad-agent-down disable-user-identity-rule
```

Example:
```
ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule
```

When the AD Agent is down and this command is configured, the ASA disables the user identity rules associated with the users in that domain. Additionally, the status of all user IP addresses in that domain is marked as disabled in the output displayed by the **show user-identity user** command. By default, this command is disabled.

**Step 11** Specify the action when a user's MAC address is found to be inconsistent with the ASA IP address currently mapped to that MAC address.

```
user-identity action mac-address-mismatch remove-user-ip
```

Example:
```
ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip
```
When this command is configured, the ASA removes the user identity-IP address mapping for that client. By default, the ASA uses the `remove-user-ip` keyword when this command is specified.

**Step 12** Define how the ASA retrieves the user identity-IP address mapping information from the AD Agent.

```
user-identity ad-agent active-user-database (on-demand | full-download)
```

Example:
```
ciscoasa(config)# user-identity ad-agent active-user-database full-download
```

By default, the ASA uses the **full-download** option.

- **Full-download**—Specifies that the ASA send a request to the AD Agent to download the entire IP-user mapping table when the ASA starts and then to receive incremental IP-user mapping information when users log in and log out. Full downloads are event driven, meaning that when there are subsequent requests to download the database, just the updates to the user identity-IP address mapping database are sent.

- **On-demand**—Specifies that the ASA retrieve the user mapping information of an IP address from the AD Agent when the ASA receives a packet that requires a new connection, and the user of its source IP address is not in the user-identity database.

When the ASA registers a change request with the AD Agent, the AD Agent sends a new event to the ASA.

**Step 13** Define the hello timer between the ASA and the AD Agent.

```
user-identity ad-agent hello-timer seconds retry-times number
```

Example:
```
ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
```

The hello timer between the ASA and the AD Agent defines how frequently the ASA exchanges hello packets. The ASA uses the hello packet to obtain ASA replication status (in-sync or out-of-sync) and domain status (up or down). If the ASA does not receive a response from the AD Agent, it resends a hello packet after the specified interval.

By default, the hello timer is set to 30 seconds and 5 retries.

**Step 14** Enable the ASA to keep track of the last event time stamp that it receives for each identifier and to discard any message if the event time stamp is at least 5 minutes older than the ASA’s clock, or if its time stamp is earlier than the last event’s time stamp.

```
user-identity ad-agent event-timestamp-check
```

Example:
```
ciscoasa(config)# user-identity ad-agent event-timestamp-check
```

For a newly booted ASA that does not have knowledge of the last event time stamp, the ASA compares the event time stamp with its own clock. If the event is at least 5 minutes older, the ASA does not accept the message.

We recommend that you configure the ASA, Active Directory, and Active Directory agent to synchronize their clocks among themselves using NTP.

**Step 15** Define the server group of the AD Agent.

```
user-identity ad-agent aaa-server aaa_server_group_tag
```

Example:
```
ciscoasa(config)# user-identity ad-agent aaa-server adagent
```
Configure Identity-Based Security Policy

You can incorporate identity-based policy in many ASA features. Any feature that uses extended ACLs (other than those listed as unsupported in the Guidelines for the Identity Firewall, page 32-7) can take advantage of an identity firewall. You can now add user identity arguments to extended ACLs, as well as network-based parameters.

Features that can use identity include the following:

- **Access rules**—An access rule permits or denies traffic on an interface using network information. With an identity firewall, you can control access based on user identity. See the firewall configuration guide.

- **AAA rules**—An authentication rule (also known as cut-through proxy) controls network access based on the user. Because this function is very similar to an access rule plus an identity firewall, AAA rules can now be used as a backup method of authentication if a user’s AD login expires. For example, for any user without a valid login, you can trigger a AAA rule. To ensure that the AAA rule is only triggered for users that do not have valid logins, you can specify special usernames in the extended ACL used for the access rule and for the AAA rule: None (users without a valid login) and Any (users with a valid login). In the access rule, configure your policy as usual for users and groups, but then include a AAA rule that permits all None users; you must permit these users so they can later trigger a AAA rule. Then, configure a AAA rule that denies Any users (these users are not subject to the AAA rule, and were handled already by the access rule), but permits all None users. For example:

  ```
  access-list 100 ex permit ip user CISCO\xyz any any
  access-list 100 ex deny ip user CISCO\abc any any
  access-list 100 ex permit ip user NONE any any
  access-list 100 ex deny any any
  access-group 100 in interface inside
  access-list 200 ex deny ip user ANY any any
  access-list 200 ex permit user NONE any any
  aaa authenticate match 200 inside user-identity
  ```

  For more information, see the legacy feature guide.

- **Cloud Web Security**—You can control which users are sent to the Cloud Web Security proxy server. In addition, you can configure policy on the Cloud Web Security ScanCenter that is based on user groups that are included in ASA traffic headers sent to Cloud Web Security. See the firewall configuration guide.

- **VPN filter**—Although a VPN does not support identity firewall ACLs in general, you can configure the ASA to enforce identity-based access rules on VPN traffic. By default, VPN traffic is not subject to access rules. You can force VPN clients to abide by access rules that use an identity firewall ACL (with the `no sysopt connection permit-VPN` command). You can also use an identity firewall ACL with the VPN filter feature; a VPN filter accomplishes a similar effect by allowing access rules in general.

**Related Topics**

- Chapter 18, “Access Control Lists.”
- Configure Local User Groups, page 17-7
Collect User Statistics

To activate the collection of user statistics by the Modular Policy Framework and match lookup actions for the Identity Firewall, perform the following steps:

Procedure

Step 1  Activate the collection of user statistics by the Modular Policy Framework and matches lookup actions for the Identify Firewall.

```
user-statistics [accounting | scanning]
```

Example:

```
ciscoasa(config)# class-map c-identity-example-1
ciscoasaciscoasa(config-cmap)# match access-list identity-example-1
ciscoasaciscoasa(config-cmap)# exit

ciscoasaciscoasa(config)# policy-map p-identity-example-1
ciscoasaciscoasa(config-pmap)# class c-identity-example-1

ciscoasaciscoasa(config-pmap)# user-statistics accounting

ciscoasaciscoasa(config-pmap)# exit

ciscoasaciscoasa(config)# service-policy p-identity-example-1 interface outside
```

The `accounting` keyword specifies that the ASA collect the sent packet count, sent drop count, and received packet count. The `scanning` keyword specifies that the ASA collect only the sent drop count.

When you configure a policy map to collect user statistics, the ASA collects detailed statistics for selected users. When you specify the `user-statistics` command without the `accounting` or `scanning` keywords, the ASA collects both accounting and scanning statistics.

Examples for the Identity Firewall

This section includes examples for configuring the Identity Firewall.

- AAA Rule and Access Rule Example 1, page 32-19
- AAA Rule and Access Rule Example 2, page 32-20
- VPN Filter Example, page 32-20

AAA Rule and Access Rule Example 1

This example shows a typical cut-through proxy configuration to allow a user to log in through the ASA. In this example, the following conditions apply:

- The ASA IP address is 172.1.1.118.
- The Active Directory domain controller has the IP address 71.1.2.93.
- The end-user client has the IP address 172.1.1.118 and uses HTTPS to log in through a web portal.
- The user is authenticated by the Active Directory domain controller via LDAP.
- The ASA uses the inside interface to connect to the Active Directory domain controller on the corporate network.
AAA Rule and Access Rule Example 2

In this example, the following guidelines apply:

- In access list commands, permit user NONE rules should be written before entering the access-list 100 ex deny any any command to allow unauthenticated incoming users to trigger AAA cut-through proxy.
- In the auth access-list command, permit user NONE rules guarantee only unauthenticated trigger cut-through proxy. Ideally, they should be the last lines.

VPN Filter Example

Some traffic might need to bypass the Identity Firewall.

The ASA reports users logging in through VPN authentication or a web portal (cut-through proxy) to the AD Agent, which distributes the user information to all registered ASA devices. Specifically, the IP-user mapping of authenticated users is forwarded to all ASA contexts that include the input interface where HTTP/HTTPS packets are received and authenticated. The ASA designates users logging in through a VPN as belonging the LOCAL domain.

There are two different ways to apply identity firewall (IDFW) rules to VPN users:

- Apply VPN-Filter with bypassing access-list check disabled
- Apply VPN-Filter with bypassing access-list check enabled
VPN with IDFW Rule -1 Example

By default, the `sysopt connection permit-vpn` command is enabled and VPN traffic is exempted from an access list check. To apply interface-based ACL rules for VPN traffic, VPN traffic access list bypassing needs to be disabled.

In this example, if the user logs in from the outside interface, the IDFW rules control which network resources are accessible. All VPN users are to be stored under the LOCAL domain. Therefore, it is only meaningful to apply the rules for LOCAL users or object groups that include LOCAL users.

```
! Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```

VPN with IDFW Rule -2 Example

By default, the `sysopt connection permit-vpn` command is enabled, with VPN traffic access bypassing enabled. A VPN filter can be used to apply the IDFW rules to the VPN traffic. A VPN filter with IDFW rules can be defined in the CLI username and group policy.

In the example, when user idfw logs in, the user can access network resources in the 10.0.00/24 subnet. However, when user user1 logs in, access to network resources in 10.0.00/24 subnet is denied. Note that all VPN users are stored under the LOCAL domain. Therefore, it is only meaningful to apply the rules for LOCAL users or object groups that include LOCAL users.

```
! Apply VPN-Filter with bypassing access-list check enabled
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v2 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
username user1 password QkBIIYVi6IFLEsYv encrypted privilege 0 username user1 attributes
  vpn-group-policy group1 vpn-filter value v2
username idfw password eEm2dmjMaopcGozT encrypted
username idfw attributes
  vpn-group-policy testgroup vpn-filter value v1
sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0 access-list v1 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0 group-policy group1 internal
v1 internal
  group-policy group1 attributes
  vpn-filter value v1
  vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
```

Monitoring the Identity Firewall

See the following commands for monitoring the Identity Firewall status:

- `show user-identity ad-agent`
This command shows the status of the AD Agent and the domains.

- `show user-identity ad-agent statistics`
  This command shows the statistics for the AD Agent.

- `show user-identity memory`
  This command shows the memory usage of various modules in the Identity Firewall.

- `show user-identity user all list`
  This command shows information about all users contained in the IP-user mapping database used by the Identity Firewall.

- `show user-identity user active user domain\user-name list detail`
  This command shows additional information about an active user.

- `show user-identity group`
  This command shows the list of user groups configured for the Identity Firewall.

### History for the Identity Firewall

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Firewall</td>
<td>8.4(2)</td>
<td>The Identity Firewall feature was introduced. We introduced or modified the following commands: <code>user-identity enable</code>, <code>user-identity default-domain</code>, <code>user-identity domain</code>, <code>user-identity logout-probe</code>, <code>user-identity inactive-user-timer</code>, <code>user-identity poll-import-user-group-timer</code>, <code>user-identity action netbios-response-fail</code>, <code>user-identity user-not-found</code>, <code>user-identity action ad-agent-down</code>, <code>user-identity action mac-address-mismatch</code>, <code>user-identity action domain-controller-down</code>, <code>user-identity ad-agent active-user-database</code>, <code>user-identity ad-agent hello-timer</code>, <code>user-identity ad-agent aaa-server</code>, <code>user-identity update import-user</code>, <code>user-identity static user</code>, <code>dns domain-lookup</code>, <code>dns poll-timer</code>, <code>dns expire-entry-timer</code>, <code>object-group user</code>, <code>show user-identity</code>, <code>show dns</code>, <code>clear configure user-identity</code>, <code>clear dns</code>, <code>debug user-identity</code>.</td>
</tr>
</tbody>
</table>
ASA and Cisco TrustSec

This chapter describes how to integrate the ASA with Cisco TrustSec.

- About Cisco TrustSec, page 33-1
- Guidelines for Cisco TrustSec, page 33-11
- Configure the AAA Server for Cisco TrustSec Integration, page 33-13
- Example for Cisco TrustSec, page 33-25
- AnyConnect VPN Support for Cisco TrustSec, page 33-26
- History for Cisco TrustSec, page 33-28

About Cisco TrustSec

Traditionally, security features such as firewalls performed access control based on predefined IP addresses, subnets, and protocols. However, with enterprises transitioning to borderless networks, both the technology used to connect people and organizations and the security requirements for protecting data and networks have evolved significantly. Endpoints are becoming increasingly nomadic and users often employ a variety of endpoints (for example, laptop versus desktop, smart phone, or tablet), which means that a combination of user attributes plus endpoint attributes provide the key characteristics (in addition to existing 6-tuple based rules), that enforcement devices such as switches and routers with firewall features or dedicated firewalls can reliably use for making access control decisions.

As a result, the availability and propagation of endpoint attributes or client identity attributes have become increasingly important requirements to enable security across the customers’ networks, at the access, distribution, and core layers of the network, and in the data center.

Cisco TrustSec provides access control 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 feature, enforcement devices use a combination of user attributes and endpoint attributes to make role-based and identity-based access control decisions. The availability and propagation of this information enables security across networks at the access, distribution, and core layers of the network.

Implementing Cisco TrustSec into your environment has the following advantages:

- Provides a growing mobile and complex workforce with appropriate and more secure access from any device
- Lowers security risks by providing comprehensive visibility of who and what is connecting to the wired or wireless network
About Cisco TrustSec

- Offers exceptional control over activity of network users accessing physical or cloud-based IT resources
- Reduces total cost of ownership through centralized, highly secure access policy management and scalable enforcement mechanisms
- For more information, see the following URLs:

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>

About SGT and SXP Support in Cisco TrustSec

In the Cisco TrustSec feature, security group access transforms a topology-aware network into a role-based network, which enables end-to-end policies enforced on the basis of role-based access control (RBAC). Device and user credentials acquired during authentication are used to classify packets by security groups. Every packet entering the Cisco TrustSec cloud is tagged with a security group tag (SGT). The tagging helps trusted intermediaries identify the source identity of the packet and enforce security policies along the data path. An SGT can indicate a privilege level across the domain when the SGT is used to define a security group ACL.

An SGT is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB), which occurs with a RADIUS vendor-specific attribute. An SGT can be assigned statically to a particular IP address or to a switch interface. An SGT is passed along dynamically to a switch or access point after successful authentication.

The Security-group eXchange Protocol (SXP) is a protocol developed for Cisco TrustSec to propagate the IP-to-SGT mapping database across network devices that do not have SGT-capable hardware support to hardware that supports SGTs and security group ACLs. SXP, a control plane protocol, passes IP-SGT mapping from authentication points (such as legacy access layer switches) to upstream devices in the network.

The SXP connections are point-to-point and use TCP as the underlying transport protocol. SXP uses the well-known TCP port number 64999 to initiate a connection. Additionally, an SXP connection is uniquely identified by the source and destination IP addresses.
Roles in the Cisco TrustSec Feature

To provide identity and policy-based access enforcement, the Cisco TrustSec feature includes the following roles:

- **Access Requester (AR)**—Access requesters are endpoint devices that request access to protected resources in the network. They are primary subjects of the architecture and their access privilege depends on their Identity credentials.

  Access requesters include endpoint devices such as PCs, laptops, mobile phones, printers, cameras, and MACsec-capable IP phones.

- **Policy Decision Point (PDP)**—A policy decision point is responsible for making access control decisions. The PDP provides features such as 802.1x, MAB, and web authentication. The PDP supports authorization and enforcement through VLAN, DACL, and security group access (SGACL/SXP/SGT).

  In the Cisco TrustSec feature, the Cisco Identity Services Engine (ISE) acts as the PDP. The Cisco ISE provides identity and access control policy functionality.

- **Policy Information Point (PIP)**—A policy information point is a source that provides external information (for example, reputation, location, and LDAP attributes) to policy decision points.

  Policy information points include devices such as Session Directory, Sensor IPS, and Communication Manager.

- **Policy Administration Point (PAP)**—A policy administration point defines and inserts policies into the authorization system. The PAP acts as an identity repository by providing Cisco TrustSec tag-to-user identity mapping and Cisco TrustSec tag-to-server resource mapping.

  In the Cisco TrustSec feature, the Cisco Secure Access Control System (a policy server with integrated 802.1x and SGT support) acts as the PAP.

- **Policy Enforcement Point (PEP)**—A policy enforcement point is the entity that carries out the decisions (policy rules and actions) made by the PDP for each AR. PEP devices learn identity information through the primary communication path that exists across networks. PEP devices learn the identity attributes of each AR from many sources, such as endpoint agents, authorization servers, peer enforcement devices, and network flows. In turn, PEP devices use SXP to propagate IP-SGT mapping to mutually trusted peer devices across the network.

  Policy enforcement points include network devices such as Catalyst switches, routers, firewalls (specifically the ASA), servers, VPN devices, and SAN devices.

  The Cisco ASA serves the PEP role in the identity architecture. Using SXP, the ASA learns identity information directly from authentication points and uses it to enforce identity-based policies.

Security Group Policy Enforcement

Security policy enforcement is based on security group name. An endpoint device attempts to access a resource in the data center. Compared to traditional IP-based policies configured on firewalls, identity-based policies are configured based on user and device identities. For example, mktg-contractor is allowed to access mktg-servers; mktg-corp-users are allowed to access mktg-server and corp-servers.

The benefits of this type of deployment include the following:

- User group and resource are defined and enforced using single object (SGT) simplified policy management.
• User identity and resource identity are retained throughout the Cisco TrustSec-capable switch infrastructure.

Figure 33-1 show a deployment for security group name-based policy enforcement.

Figure 33-1 Security Group Name-Based Policy Enforcement Deployment

Implementing Cisco TrustSec allows you to configure security policies that support server segmentation and includes the following features:

• A pool of servers can be assigned an SGT for simplified policy management.
• The SGT information is retained within the infrastructure of Cisco TrustSec-capable switches.
• The ASA can use the IP-SGT mapping for policy enforcement across the Cisco TrustSec domain.
• Deployment simplification is possible because 802.1x authorization for servers is mandatory.

How the ASA Enforces Security Group-Based Policies

User-based security policies and security-group based policies can coexist on the ASA. Any combination of network, user-based, and security-group based attributes can be configured in a security policy.

To configure the ASA to function with Cisco TrustSec, you must import a Protected Access Credential (PAC) file from the ISE.

Importing the PAC file to the ASA establishes a secure communication channel with the ISE. After the channel is established, the ASA initiates a PAC secure RADIUS transaction with the ISE and downloads Cisco TrustSec environment data (that is, the security group table). The security group table maps SGTs to security group names. Security group names are created on the ISE and provide user-friendly names for security groups.

The first time that the ASA downloads the security group table, it walks through all entries in the table and resolves all the security group names included in security policies that have been configured on it; then the ASA activates those security policies locally. If the ASA cannot resolve a security group name, it generates a syslog message for the unknown security group name.
Figure 33-2 shows how a security policy is enforced in Cisco TrustSec.

**Figure 33-2  Security Policy Enforcement**

1. An endpoint device connects to an access layer device directly or via remote access and authenticates with Cisco TrustSec.

2. The access layer device authenticates the endpoint device with the ISE by using authentication methods such as 802.1X or web authentication. The endpoint device passes role and group membership information to classify the device into the appropriate security group.

3. The access layer device uses SXP to propagate the IP-SGT mapping to the upstream devices.

4. The ASA receives the packet and looks up the SGTs for the source and destination IP addresses using the IP-SGT mapping passed by SXP.

   If the mapping is new, the ASA records it in its local IP-SGT Manager database. The IP-SGT Manager database, which runs in the control plane, tracks IP-SGT mapping for each IPv4 or IPv6 address. The database records the source from which the mapping was learned. The peer IP address of the SXP connection is used as the source of the mapping. Multiple sources can exist for each IP-SGT mapped entry.

   If the ASA is configured as a Speaker, the ASA transmits all IP-SGT mapping entries to its SXP peers.

5. If a security policy is configured on the ASA with that SGT or security group name, the ASA enforces the policy. (You can create security policies on the ASA that include SGTs or security group names. To enforce policies based on security group names, the ASA needs the security group table to map security group names to SGTs.)

   If the ASA cannot find a security group name in the security group table and it is included in a security policy, the ASA considers the security group name to be unknown and generates a syslog message. After the ASA refreshes the security group table from the ISE and learns the security group name, the ASA generates a syslog message indicating that the security group name is known.

**Effects of Changes to Security Groups on the ISE**

The ASA periodically refreshes the security group table by downloading an updated table from the ISE. Security groups can change on the ISE between downloads. These changes are not reflected on the ASA until it refreshes the security group table.
About Cisco TrustSec

We recommend that you schedule policy configuration changes on the ISE during a maintenance window, then manually refresh the security group table on the ASA to make sure the security group changes have been incorporated.

Handling policy configuration changes in this way maximizes the chances of security group name resolution and immediate activation of security policies.

The security group table is automatically refreshed when the environment data timer expires. You can also trigger a security group table refresh on demand.

If a security group changes on the ISE, the following events occur when the ASA refreshes the security group table:

- Only security group policies that have been configured using security group names need to be resolved with the security group table. Policies that include security group tags are always active.
- When the security group table is available for the first time, all policies with security group names are walked through, security group names are resolved, and policies are activated. All policies with tags are walked through, and syslogs are generated for unknown tags.
- If the security group table has expired, policies continue to be enforced according to the most recently downloaded security group table until you clear it, or a new table becomes available.
- When a resolved security group name becomes unknown on the ASA, it deactivates the security policy; however, the security policy persists in the ASA running configuration.
- If an existing security group is deleted on the PAP, a previously known security group tag can become unknown, but no change in policy status occurs on the ASA. A previously known security group name can become unresolved, and the policy is then inactivated. If the security group name is reused, the policy is recompiled using the new tag.
- If a new security group is added on the PAP, a previously unknown security group tag can become known, a syslog message is generated, but no change in policy status occurs. A previously unknown security group name can become resolved, and associated policies are then activated.
- If a tag has been renamed on the PAP, policies that were configured using tags display the new name, and no change in policy status occurs. Policies that were configured with security group names are recompiled using the new tag value.

Speaker and Listener Roles on the ASA

The ASA supports SXP to send and receive IP-SGT mapping entries to and from other network devices. Using SXP allows security devices and firewalls to learn identity information from access switches without the need for hardware upgrades or changes. SXP can also be used to pass IP-SGT mapping entries from upstream devices (such as data center devices) back to downstream devices. The ASA can receive information from both upstream and downstream directions.

When configuring an SXP connection on the ASA to an SXP peer, you must designate the ASA as a Speaker or a Listener for that connection so that it can exchange Identity information:

- Speaker mode—Configures the ASA so that it can forward all active IP-SGT mapping entries collected on the ASA to upstream devices for policy enforcement.
- Listener mode—Configures the ASA so that it can receive IP-SGT mapping entries from downstream devices (SGT-capable switches) and use that information to create policy definitions.
If one end of an SXP connection is configured as a Speaker, then the other end must be configured as a Listener, and vice versa. If both devices on each end of an SXP connection are configured with the same role (either both as Speakers or both as Listeners), the SXP connection fails and the ASA generates a syslog message.

Multiple SXP connections can learn IP-SGT mapping entries that have been downloaded from the IP-SGT mapping database. After an SXP connection to an SXP peer is established on the ASA, the Listener downloads the entire IP-SGT mapping database from the Speaker. All changes that occur after this are sent only when a new device appears on the network. As a result, the rate of SXP information flow is proportional to the rate at which end hosts authenticate to the network.

IP-SGT mapping entries that have been learned through SXP connections are maintained in the SXP IP-SGT mapping database. The same mapping entries may be learned through different SXP connections. The mapping database maintains one copy for each mapping entry learned. Multiple mapping entries of the same IP-SGT mapping value are identified by the peer IP address of the connection from which the mapping was learned. SXP requests that the IP-SGT Manager add a mapping entry when a new mapping is learned the first time and remove a mapping entry when the last copy in the SXP database is removed.

Whenever an SXP connection is configured as a Speaker, SXP requests that the IP-SGT Manager forward all the mapping entries collected on the device to the peer. When a new mapping is learned locally, the IP-SGT Manager requests that SXP forward it through connections that are configured as Speakers.

Configuring the ASA to be both a Speaker and a Listener for an SXP connection can cause SXP looping, which means that SXP data can be received by an SXP peer that originally transmitted it.

**SXP Chattiness**

The rate of SXP information flow is proportional to the rate at which end hosts authenticate into the network. After an SXP peering is established, the listener device downloads the entire IP-SGT database from the speaker device. After that, all changes are sent incrementally only when a new device appears on the network or leaves the network. Also, note that only access devices that are attached to the new device initiate this incremental update to the upstream device.

In other words, SXP protocol is no chattier than the authentication rate, which is limited to the capability of the authentication server. Therefore, SXP chattiness is not a major concern.

**SXP Timers**

- **Retry Open Timer**—The retry open timer is triggered if one SXP connection on the device is not up. After the retry open timer expires, the device goes through the entire connection database and if any connection is in the off or “pending on” state, the retry open timer restarts. The default timer value is 120 seconds. A zero value means the retry timer does not start. The retry open timer continues until all the SXP connections are set up, or the retry open timer has been configured to be 0.

- **Delete Hold-Down Timer**—The connection-specific delete hold-down timer is triggered when a connection on the Listener is torn down. The mapping entries that have been learned are not deleted immediately, but are held until the delete hold-down timer expires. The mapping entries are deleted after this timer expires. The delete hold-down timer value is set to 120 seconds and is not configurable.

- **Reconciliation Timer**—If an SXP connection is brought up within the delete hold-down timer period, a bulk update is performed on this connection. This means that the most recent mapping entries are learned and are associated with a new connection instantiation identifier. A periodic,
connection-specific reconciliation timer starts in the background. When this reconciliation timer expires, it scans the entire SXP mapping database and identifies all mapping entries that have not been learned in the current connection session (that is, mapping entries with an unmatched connection instantiation identifier), and marks them for deletion. These entries are deleted in the subsequent reconciliation review. The default reconciliation timer value is 120 seconds. A zero value is not allowed on the ASA to prevent obsolete entries from staying for an unspecified length of time and causing unexpected results in policy enforcement.

- **HA Reconciliation Timer**—When HA is enabled, the SXP mapping database of the active and standby units are in sync. The new active unit tries to establish new SXP connections to all its peers and acquires the latest mapping entries. An HA reconciliation timer provides a way of identifying and removing old mapping entries. It starts after a failover occurs, which gives the ASA time to acquire the latest mapping entries. After the HA reconciliation timer expires, the ASA scans the entire SXP mapping database and identifies all the mapping entries have not been learned in the current connection session. Mapping entries with unmatched instantiation identifiers are marked for deletion. This reconciliation mechanism is the same as that of the reconciliation timer. The time value is the same as the reconciliation timer and is configurable.

After an SXP peer terminates its SXP connection, the ASA starts a delete hold-down timer. Only SXP peers designated as Listeners can terminate a connection. If an SXP peer connects while the delete hold-down timer is running, the ASA starts the reconciliation timer; then the ASA updates the IP-SGT mapping database to learn the most recent mapping.

**IP-SGT Manager Database**

The IP-SGT Manager database does not synchronize any entries from the active unit to the standby unit. Each source from which the IP-SGT Manager database receives IP-SGT mapping entries synchronizes its database from the active unit to the standby unit, then provides the final IP-SGT mapping to the IP-SGT Manager on the standby unit.

For Version 9.0(1), the IP-SGT Manager database receives IP-SGT mapping updates from the SXP source only.

**Features of the ASA-Cisco TrustSec Integration**

Cisco TrustSec provides the following capabilities:

**Flexibility**

- The ASA can be configured as an SXP Speaker or Listener, or both.
- The ASA supports SXP for IPv6 and IPv6-capable network devices.
- SXP can change mapping entries for IPv4 and IPv6 addresses.
- SXP endpoints support IPv4 and IPv6 addresses.
- The ASA supports SXP Version 2 only.
- The ASA negotiates SXP versions with different SXP-capable network devices. SXP version negotiation eliminates the need for static configuration of versions.
- You can configure the ASA to refresh the security group table when the SXP reconcile timer expires and you can download the security group table on demand. When the security group table on the ASA is updated from the ISE, changes are reflected in the appropriate security policies.
The ASA supports security policies based on security group names in the source or destination fields, or both. You can configure security policies on the ASA based on combinations of security groups, IP address, Active Directory group/user name, and FQDN.

**Availability**

- You can configure security group-based policies on the ASA in both the Active/Active and Active/Standby configurations.
- The ASA can communicate with the ISE configured for high availability (HA).
- You can configure multiple ISE servers on the ASA and if the first server is unreachable, it continues to the next server, and so on. However, if the server list is downloaded as part of the Cisco TrustSec environment data, it is ignored.
- If the PAC file downloaded from the ISE expires on the ASA and it cannot download an updated security group table, the ASA continues to enforce security policies based on the last downloaded security group table until the ASA downloads an updated table.

**Clustering**

- For Layer 2 networks, all units share the same IP address. When you change the interface address, the changed configuration is sent to all other units. When the IP address is updated from the interface of a particular unit, a notification is sent to update the IP-SGT local database on this unit.
- For Layer 3 networks, a pool of addresses is configured for each interface on the master unit, and this configuration is synchronized to the slave units. On the master unit, a notification of the IP addresses that have been assigned to the interface is sent, and the IP-SGT local database is updated. The IP-SGT local database on each slave unit can be updated with the IP address information for the master unit by using the address pool configuration that has been synchronized to it, where the first address in the pool for each interface always belongs to the master unit.

When a slave unit boots, it notifies the master unit. Then the master unit goes through the address pool on each interface and computes the IP address for the new slave unit that sent it the notification, and updates the IP-SGT local database on the master unit. The master unit also notifies the other slave units about the new slave unit. As part of this notification processing, each slave unit computes the IP address for the new slave unit and adds this entry to the IP-SGT local database on each slave unit. All the slave units have the address pool configuration to determine the IP address value. For each interface, the value is determined as follows:

Master IP + (M-N), where:

- **M**—Maximum number of units (up to 8 are allowed)
- **N**—Slave unit number that sent the notification

When the IP address pool changes on any interface, the IP addresses for all the slave units and the master unit need to be recalculated and updated in the IP-SGT local database on the master unit, as well as on every other slave unit. The old IP address needs to be deleted, and the new IP address needs to be added.

When this changed address pool configuration is synchronized to the slave unit, as a part of configuration change processing, each slave unit recomputes the IP address for the master unit and for every other slave unit whose IP address has changed, then removes the entry for the old IP address and adds the new IP address.
About Cisco TrustSec

Scalability

Table 33-1 show the number of IP-SGT mapping entries that the ASA supports.

<table>
<thead>
<tr>
<th>ASA Model</th>
<th>Number of IP-SGT Mapping Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>5585-X with SSP-10</td>
<td>18,750</td>
</tr>
<tr>
<td>5585-X with SSP-20</td>
<td>25,000</td>
</tr>
<tr>
<td>5585-X with SSP-40</td>
<td>50,000</td>
</tr>
<tr>
<td>5585-X with SSP-60</td>
<td>100,000</td>
</tr>
</tbody>
</table>

Table 33-2 shows the number of SXP connections that the ASA supports.

<table>
<thead>
<tr>
<th>ASA Model</th>
<th>Number of SXP TCP Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>5585-X with SSP-10</td>
<td>150</td>
</tr>
<tr>
<td>5585-X with SSP-20</td>
<td>250</td>
</tr>
<tr>
<td>5585-X with SSP-40</td>
<td>500</td>
</tr>
<tr>
<td>5585-X with SSP-60</td>
<td>1000</td>
</tr>
</tbody>
</table>

Register the ASA with the ISE

The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can successfully import a PAC file. To register the ASA with the ISE, perform the following steps:

1. Log into the ISE.
2. Choose Administration > Network Devices > Network Devices.
3. Click Add.
4. Enter the IP address of the ASA.
5. When the ISE is being used for user authentication, enter a shared secret in the Authentication Settings area.
   When you configure the AAA sever on the ASA, provide the shared secret that you create here on the ISE. The AAA server on the ASA uses this shared secret to communicate with the ISE.
6. Specify a device name, device ID, password, and a download interval for the ASA. See the ISE documentation for how to perform these tasks.

Create a Security Group on the ISE

When configuring the ASA to communicate with the ISE, you specify a AAA server. When configuring the AAA server on the ASA, you must specify a server group. The security group must be configured to use the RADIUS protocol. To create a security group on the ISE, perform the following steps:

1. Log into the ISE.
3. Add a security group for the ASA. (Security groups are global and not ASA specific.)
   The ISE creates an entry under Security Groups with a tag.
4. In the Security Group Access area, configure device ID credentials and a password for the ASA.

**Generate the PAC File**

To generate the PAC file, perform the following steps:

1. Log into the ISE.
2. Choose Administration > Network Resources > Network Devices.
3. From the list of devices, choose the ASA.
4. Under the Security Group Access (SGA), click Generate PAC.
5. To encrypt the PAC file, enter a password.

   The password (or encryption key) that you enter to encrypt the PAC file is independent of the password that was configured on the ISE as part of the device credentials.

   The ISE generates the PAC file. The ASA can import the PAC file from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC file does not have to reside on the ASA flash before you can import it.)

   **Note**
   
   The PAC file includes a shared key that allows the ASA and ISE to secure the RADIUS transactions that occur between them. For this reason, make sure that you store it securely on the ASA.

**Guidelines for Cisco TrustSec**

**Failover**

- Supports a list of servers via configuration. If the first server is unreachable, the ASA tries to contact the second server in the list, and so on. However, the server list downloaded as part of the Cisco TrustSec environment data is ignored.
- When the ASA is part of a failover configuration, you must import the PAC file to the primary ASA device.
- When the ASA is part of a failover configuration, you must refresh the environment data on the primary ASA device.

**Clustering**

- When the ASA is part of a clustering configuration, you must import the PAC file to the master unit.
- When the ASA is part of a clustering configuration, you must refresh the environment data on the master unit.

**IPv6**

The ASA supports SXP for IPv6 and IPv6-capable network devices. The AAA server must use an IPv4 address.
Layer 2 SGT Imposition

- Supported only on physical interfaces, VLAN interfaces, port channel interfaces, and redundant interfaces.
- Not supported on logical interfaces or virtual interfaces, such as BVI.
- Does not support link encryption using SAP negotiation and MACsec.
- Not supported on failover links.
- Not supported on cluster control links.
- The ASA does not reclassify existing flows if the SGT is changed. Any policy decisions that were made based on the previous SGT remain in force for the life of the flow. However, the ASA can immediately reflect SGT changes on egress packets, even if the packets belong to a flow whose classification was based on a previous SGT.
- The hardware architecture of the ASA 5585-X is designed to load balance regular packets in an optimal way, but this is not the case for inline tagged packets with Layer 2 Security Group Tagging Imposition. Significant performance degradation on the ASA 5585-X may occur when it processes incoming inline tagged packets. This issue does not occur with inline tagged packets on other ASA platforms, as well as with untagged packets on the ASA 5585-X. One workaround is to offload access policies so that minimal inline tagged packets go to the ASA 5585-X, which allows the switches to handle tagged policy enforcement. Another workaround is to use SXP so that the ASA 5585-X can map the IP address to the security group tag without the need to receive tagged packets.
- The ASASM does not support Layer 2 Security Group Tagging Imposition.

Additional Guidelines

- Cisco TrustSec supports the Smart Call Home feature in single context and multi-context mode, but not in the system context.
- The ASA can only be configured to interoperate in a single Cisco TrustSec domain.
- The ASA does not support static configuration of SGT-name mapping on the device.
- NAT is not supported in SXP messages.
- SXP conveys IP-SGT mapping to enforcement points in the network. If an access layer switch belongs to a different NAT domain than the enforcing point, the IP-SGT map that it uploads is invalid, and an IP-SGT mapping database lookup on the enforcement device does not yield valid results. As a result, the ASA cannot apply security group-aware security policy on the enforcement device.
- You can configure a default password for the ASA to use for SXP connections, or you can choose not to use a password; however, connection-specific passwords are not supported for SXP peers. The configured default SXP password should be consistent across the deployment network. If you configure a connection-specific password, connections may fail and a warning message appears. If you configure the connection with the default password, but it is not configured, the result is the same as when you have configured the connection with no password.
- SXP connection loops can form when a device has bidirectional connections to a peer or is part of a unidirectionally connected chain of devices. (The ASA can learn IP-SGT mapping for resources from the access layer in the data center. The ASA might need to propagate these tags to downstream devices.) SXP connection loops can cause unexpected behavior of SXP message transport. In cases where the ASA is configured to be a Speaker and Listener, an SXP connection loop can occur, causing SXP data to be received by the peer that originally transmitted it.
- When changing the ASA local IP address, you must ensure that all SXP peers have updated their peer list. In addition, if SXP peers changes its IP addresses, you must ensure those changes are reflected on the ASA.
Automatic PAC file provisioning is not supported. The ASA administrator must request the PAC file from the ISE administrative interface and import it into the ASA.

PAC files have expiration dates. You must import the updated PAC file before the current PAC file expires; otherwise, the ASA cannot retrieve environment data updates.

When a security group changes on the ISE (for example, it is renamed or deleted), the ASA does not change the status of any ASA security policies that contain an SGT or security group name associated with the changed security group; however, the ASA generates a syslog message to indicate that those security policies changed.

The multi-cast types are not supported in ISE 1.0.

An SXP connection stays in the initializing state among two SXP peers interconnected by the ASA; as shown in the following example:

(SXP peer A) - - - - (ASA) - - - (SXP peer B)

Therefore, when configuring the ASA to integrate with Cisco TrustSec, you must enable the no-NAT, no-SEQ-RAND, and MD5-AUTHENTICATION TCP options on the ASA to configure SXP connections. Create a TCP state bypass policy for traffic destined to SXP port TCP 64999 among the SXP peers. Then apply the policy on the appropriate interfaces.

For example, the following set of commands shows how to configure the ASA for a TCP state bypass policy:

```plaintext
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
match access-list SXP-MD5-ACL

class-map SXP-MD5-CLASSMAP
match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
parameters
    message-length maximum 512

policy-map global_policy
class SXP-MD5-CLASSMAP
    set connection random-sequence-number disable
    set connection advanced-options SXP-MD5-OPTION-ALLOW
    set connection advanced-options tcp-state-bypass

service-policy global_policy global
```

Configure the AAA Server for Cisco TrustSec Integration

This section describes how to configure the AAA server for Cisco TrustSec integration.

Before You Begin

- The referenced server group must be configured to use the RADIUS protocol. If you add a non-RADIUS server group to the ASA, the configuration fails.
- If the ISE is also used for user authentication, obtain the shared secret that was entered on the ISE when you registered the ASA with the ISE. Contact your ISE administrator to obtain this information.
To configure the AAA server group to communicate with the ISE on the ASA, perform the following steps:

**Procedure**

**Step 1** Create the AAA server group and configure the AAA server parameters for the ASA to communicate with the ISE server.

```
aaa-server server-tag protocol radius
```

Example:
```
ciscoasa(config)# aaa-server ISEserver protocol radius
```

The *server-tag* argument specifies the server group name.

**Step 2** Exit from the aaa server group configuration mode.

```
exit
```

Example:
```
ciscoasa(config-aaa-server-group)# exit
```

**Step 3** Configure a AAA server as part of a AAA server group and set host-specific connection data.
```
ciscoasa(config)# aaa-server server-tag (interface-name) host server-ip
```

Example:
```
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
```

The *interface-name* argument specifies the network interface where the ISE server resides. The parentheses are required in this parameter. The *server-tag* argument is the name of the AAA server group. The *server-ip* argument specifies the IP address of the ISE server.

**Step 4** Specify the server secret value used to authenticate the ASA with the ISE server.
```
key key
```

Example:
```
ciscoasa(config-aaa-server-host)# key myexclusivekey
```

The *key* argument is an alphanumeric keyword up to 127 characters long. If the ISE is also used for user authentication, enter the shared secret that was entered on the ISE when you registered the ASA with the ISE.

**Step 5** Exit from the aaa server host configuration mode.

```
exit
```

Example:
```
ciscoasa(config-aaa-server-host)# exit
```

**Step 6** Identify the AAA server group that is used by Cisco TrustSec for environment data retrieval.
```
cts server-group AAA-server-group-name
```

Example:
```
ciscoasa(config)# cts server-group ISEserver
```
The `AAA-server-group-name` argument is the name of the AAA server group that you specified in Step 1 in the `server-tag` argument.

**Note** You may configure only one instance of the server group on the ASA for Cisco TrustSec.

**Examples**
The following example shows how to configure the ASA to communicate with the ISE server for Cisco TrustSec integration:

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

### Step 7

**Import a PAC File**

This section describes how to import a PAC file.

**Before You Begin**
- The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can generate a PAC file.
- Obtain the password used to encrypt the PAC file when generating it on the ISE. The ASA requires this password to import and decrypt the PAC file.
- The ASA requires access to the PAC file generated by the ISE. The ASA can import the PAC file from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC file does not need to reside on the ASA flash before you can import it.)
- The server group has been configured for the ASA.

To import a PAC file, perform the following steps:

**Procedure**

### Step 1
Import a Cisco TrustSec PAC file.

```
ciscoasa(config)# cts import-pac filepath password value
```

Example:
```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

The `value` argument specifies the password used to encrypt the PAC file. The password is independent of the password that was configured on the ISE as part of the device credentials. The `filepath` argument is entered as one of the following options:

**Single Mode**
- `disk0`: Path and filename on disk0
Guidelines for Cisco TrustSec

Chapter 33      ASA and Cisco TrustSec

Examples
The following example shows how to import a PAC file into the ASA:

ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported

The following example shows how to use the terminal to import a PAC file into the ASA:

ciscoasa(config)# cts import-pac terminal password A98752a551
Enter the PAC file data in ASCII hex format
End with the word 'quit' on a line by itself.
ciscoasa(exec_pac_hex)# 01002904050000010000000000000000
...
Configure the Security Exchange Protocol

This section describes how to configure the Security Exchange Protocol.

Before You Begin
At least one interface must be in the UP/UP state.

Note
When SXP is enabled with all interfaces down, the ASA does not display a message indicating that SXP is not working or it could not be enabled. If you check the configuration by entering the `show running-config` command, the command output displays the following message:

"WARNING: SXP configuration in process, please wait for a few moments and try again."

This message is generic and does not specify the reason why SXP is not working.

To configure SXP, perform the following steps:

Procedure

Step 1  
Enable SXP on the ASA. By default, SXP is disabled.

```plaintext
cts sxp enable
```

Example:

```
ciscoasa(config)# cts sxp enable
```

Step 2  
Configure the default source IP address for SXP connections.

```plaintext
cts sxp default source-ip ipaddress
```

Example:

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

The `ipaddress` argument is an IPv4 or IPv6 address.

When you configure a default source IP address for SXP connections, you must specify the same address as the ASA outbound interface. If the source IP address does not match the address of the outbound interface, SXP connections fail.

When a source IP address for an SXP connection is not configured, the ASA performs a route/ARP lookup to determine the outbound interface for the SXP connection.

Step 3  
Configure the default password for TCP MD5 authentication with SXP peers. By default, SXP connections do not have a password.

```plaintext
cts sxp default password [0 | 8] password
```

Example:

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

Configuring an encryption level for the password is optional. If you configure an encryption level, you can only set one level:

- Level 0—unencrypted cleartext
- Level 8—encrypted text
The password argument specifies an encrypted string of up to 162 characters or an ASCII key string up to 80 characters.

**Step 4** Specify the default time interval between ASA attempts to set up new SXP connections between SXP peers.

```plaintext
ciscoasa(config)# cts sxp retry period timervalue
```

Example:

```
ciscoasa(config)# cts sxp retry period 60
```

The ASA continues to make connection attempts until a successful connection is made. The retry timer is triggered as long as there is one SXP connection on the ASA that is not up.

The timervalue argument ranges from 0 to 64000 seconds. The default is 120 seconds. If you specify 0 seconds, the timer never expires and the ASA does not try to connect to SXP peers.

When the retry timer expires, the ASA goes through the connection database and if the database contains any connections that are off or in a “pending on” state, the ASA restarts the retry timer.

We recommend that you configure the retry timer to a different value from its SXP peer devices.

**Step 5** Specify the value of the default reconcile timer.

```plaintext
ciscoasa(config)# cts sxp reconciliation period timervalue
```

Example:

```
ciscoasa(config)# cts sxp reconciliation period 60
```

After an SXP peer terminates its SXP connection, the ASA starts a hold-down timer.

If an SXP peer connects while the hold-down timer is running, the ASA starts the reconcile timer; then the ASA updates the SXP mapping database to learn the latest mapping.

When the reconcile timer expires, the ASA scans the SXP mapping database to identify stale mapping entries (which were learned in a previous connection session). The ASA marks these connections as obsolete. When the reconcile timer expires, the ASA removes the obsolete entries from the SXP mapping database.

The timervalue argument ranges from 1 to 64000 seconds. The default is 120 seconds.

You cannot specify 0 seconds for the timer, because this value prevents the reconcile timer from starting. Not allowing the reconcile timer to run would keep stale entries for an undefined time and cause unexpected results from policy enforcement.

---

**Examples**

The following example shows how to set default values for SXP:

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```
Add an SXP Connection Peer

To add an SXP connection peer, perform the following steps:

**Procedure**

**Step 1**
Enable SXP on the ASA. By default, SXP is disabled.
```
cts sxp enable
```
Example:
```
ciscoasa(config)# cts sxp enable
```

**Step 2**
Set up an SXP connection to an SXP peer.
```
cts sxp connection peer peer_ip_address [source source_ip_address] password (default | none) [mode {local | peer}] {speaker | listener}
```
Example:
```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

SXP connections are set per IP address; a single device pair can service multiple SXP connections.
The `peer_ip_address` argument is the IPv4 or IPv6 address of the SXP peer. The peer IP address must be reachable from the ASA outgoing interface.
The `source_ip_address` argument is the local IPv4 or IPv6 address of the SXP connection. The source IP address must be the same as the ASA outbound interface or the connection fails.
We recommend that you do not configure a source IP address for an SXP connection and allow the ASA to perform a route/ARP lookup to determine the source IP address for the SXP connection.

Indicate whether or not to use the authentication key for the SXP connection:
- `default`—Use the default password configured for SXP connections.
- `none`—Do not use a password for the SXP connection.

Indicate the mode of the SXP connection:
- `local`—Use the local SXP device.
- `peer`—Use the peer SXP device.

Indicate whether the ASA functions as a Speaker or Listener for the SXP connection:
- `speaker`—The ASA can forward IP-SGT mapping to upstream devices.
- `listener`—The ASA can receive IP-SGT mapping from downstream devices.

**Examples**
The following example shows how to configure SXP peers on the ASA:
```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default mode peer
no cts sxp connection peer 192.168.1.100
ciscoasa(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
no cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
```
Refresh Environment Data

The ASA downloads environment data from the ISE, which includes the Security Group Tag (SGT) name table. The ASA automatically refreshes its environment data that is obtained from the ISE when you complete the following tasks on the ASA:

- Configure a AAA server to communicate with the ISE.
- Import a PAC file from the ISE.
- Identify the AAA server group that the ASA will use to retrieve Cisco TrustSec environment data.

Normally, you do not need to manually refresh the environment data from the ISE; however, security groups can change on the ISE. These changes are not reflected on the ASA until you refresh the data in the ASA security group table, so refresh the data on the ASA to make sure that any security group changes made on the ISE are reflected on the ASA.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>We recommend that you schedule policy configuration changes on the ISE and the manual data refresh on the ASA during a maintenance window. Handling policy configuration changes in this way maximizes the chances of security group names getting resolved and security policies becoming active immediately on the ASA.</td>
</tr>
</tbody>
</table>

To refresh the environment data, perform the following steps:

**Procedure**

**Step 1**

Refresh the environment data from the ISE and reset the reconcile timer to the configured default value.

```plaintext
cts refresh environment-data
```

Example:

```plaintext
ciscoasa(config)# cts refresh environment-data
```

Configure the Security Policy

You can incorporate Cisco TrustSec policy in many ASA features. Any feature that uses extended ACLs (unless listed in this chapter as unsupported) can take advantage of Cisco TrustSec. You can add security group arguments to extended ACLs, as well as traditional network-based parameters.

- To configure an extended ACL, see the firewall configuration guide.
- To configure security group object groups that can be used in the ACL, see Configure Security Group Object Groups, page 17-8.

For example, an access rule permits or denies traffic on an interface using network information. With Cisco TrustSec, you can control access based on security group. For example, you could create an access rule for sample_securitygroup1 10.0.0.0 255.0.0.0, meaning the security group could have any IP address on subnet 10.0.0.0/8.

You can configure security policies based on combinations of security group names (servers, users, unmanaged devices, and so on), user-based attributes, and traditional IP-address-based objects (IP address, Active Directory object, and FQDN). Security group membership can extend beyond roles to include device and location attributes and is independent of user group membership.
Examples

The following example shows how to create an ACL that uses a locally defined security object group:

```
object-group security objgrp-it-admin
    security-group name it-admin-sg-name
    security-group tag 1

object-group security objgrp-hr-admin
    security-group name hr-admin-sg-name // single sg_name
    group-object it-admin // locally defined object-group as nested object

object-group security objgrp-hr-servers
    security-group name hr-servers-sg-name

object-group security objgrp-hr-network
    security-group tag 2

access-list hr-acl permit ip object-group-security objgrp-hr-admin any
    object-group-security objgrp-hr-servers

The ACL configured in the previous example can be activated by configuring an access group or the Modular Policy Framework.

Additional examples:

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
   access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53
!match src hr-admin-sg-name from host 10.1.1.1 to dst any
   access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any
!match src tag 22 from any network to dst hr-servers-sg-name any network
   access-list idfw-acl permit ip security-group tag 22 any security-group name hr-servers-sg-name any
!match src user mary from any host to dst hr-servers-sg-name any network
   access-list idfw-acl permit ip user CSCO\mary any security-group name hr-servers-sg-name any
!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
   access-list idfw-acl permit ip object-group-security objgrp-hr-admin any object-group-security
    objgrp-hr-servers any
!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24 to dst objgrp-hr-servers any network
   access-list idfw-acl permit ip user CSCO\Jack object-group-security objgrp-hr-network 10.1.1.0
   255.255.255.0 object-group-security objgrp-hr-servers any
!match src user Tom from security-group mktg any google.com
   object network net-google
   fqdn google.com
   access-list sgacl permit ip sec name mktg any object net-google
! If user Tom or object_group security objgrp-hr-admin needs to be matched, multiple ACEs can be defined as
   follows:
   access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0 object-group-security
    objgrp-hr-servers any
   access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin 10.1.1.0 255.255.255.0
   object-group-security objgrp-hr-servers any
```

Layer 2 Security Group Tagging Imposition

Cisco TrustSec identifies and authenticates each network user and resource and assigns a 16-bit number called a Security Group Tag (SGT). This identifier is in turn propagated between network hops, which allows any intermediary devices such as ASAs, switches, and routers to enforce polices based on this identity tag.

SGT plus Ethernet Tagging, also called Layer 2 SGT Imposition, enables the ASA to send and receive security group tags on Ethernet interfaces using Cisco proprietary Ethernet framing (EtherType 0x8909), which allows the insertion of source security group tags into plain-text Ethernet frames. The ASA inserts security group tags on the outgoing packet and processes security group tags on the incoming packet,
based on a manual per-interface configuration. This feature allows inline hop-by-hop propagation of endpoint identity across network devices and provides seamless Layer 2 SGT Impose between each hop.

Figure 33-3 shows a typical example of Layer 2 SGT Impose.

Figure 33-3  Layer 2 SGT Impose

Usage Scenarios

Table 33-3 describes the expected behavior for ingress traffic when configuring this feature.

Table 33-3  Ingress Traffic

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Tagged Packet Received</th>
<th>Untagged Packet Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>No command is issued.</td>
<td>Packet is dropped.</td>
<td>SGT value is from the IP-SGT Manager.</td>
</tr>
<tr>
<td>The cts manual command is issued.</td>
<td>SGT value is from the IP-SGT Manager.</td>
<td>SGT value is from the IP-SGT Manager.</td>
</tr>
<tr>
<td>The cts manual command and the policy static sgt sgt_number command are both issued.</td>
<td>SGT value is from the policy static sgt sgt_number command.</td>
<td>SGT value is from the policy static sgt sgt_number command.</td>
</tr>
<tr>
<td>The cts manual command and the policy static sgt sgt_number trusted command are both issued.</td>
<td>SGT value is from the inline SGT in the packet.</td>
<td>SGT value is from the policy static sgt sgt_number command.</td>
</tr>
</tbody>
</table>

Note: If there is no matched IP-SGT mapping from the IP-SGT Manager, then a reserved SGT value of “0x0” for “Unknown” is used.
Table 33-4 describes the expected behavior for egress traffic when configuring this feature.

### Table 33-4  Egress Traffic

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Tagged or Untagged Packet Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No command is issued.</td>
<td>Untagged</td>
</tr>
<tr>
<td>The <code>cts manual</code> command is issued.</td>
<td>Tagged</td>
</tr>
<tr>
<td>The <code>cts manual</code> command and the <code>propagate sgt</code> command are both issued.</td>
<td>Tagged</td>
</tr>
<tr>
<td>The <code>cts manual</code> command and the <code>no propagate sgt</code> command are both issued.</td>
<td>Untagged</td>
</tr>
</tbody>
</table>

Table 33-5 describes the expected behavior for to-the-box and from-the-box traffic when configuring this feature.

### Table 33-5  To-the-box and From-the-box Traffic

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Tagged or Untagged Packet Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>No command is issued on the ingress interface for to-the-box traffic.</td>
<td>Packet is dropped.</td>
</tr>
<tr>
<td>The <code>cts manual</code> command is issued on the ingress interface for to-the-box traffic.</td>
<td>Packet is accepted, but there is no policy enforcement or SGT propagation.</td>
</tr>
<tr>
<td>The <code>cts manual</code> command is not issued or the <code>cts manual</code> command and <code>no propagate sgt</code> command are both issued on the egress interface for from-the-box traffic.</td>
<td>Untagged packet is sent, but there is no policy enforcement. The SGT number is from the IP-SGT Manager.</td>
</tr>
<tr>
<td>The <code>cts manual</code> command is issued or the <code>cts manual</code> command and the <code>propagate sgt</code> command are both issued on the egress interface for from-the-box traffic.</td>
<td>Tagged packet is sent. The SGT number is from the IP-SGT Manager.</td>
</tr>
</tbody>
</table>

**Note**
If there is no matched IP-SGT mapping from the IP-SGT Manager, then a reserved SGT value of “0x0” for “Unknown” is used.

## Configure a Security Group Tag on an Interface

To configure a security group tag on an interface, perform the following steps:

**Procedure**

**Step 1**
Specify an interface and enter interface configuration mode.

```
icontext id
```

Example:
```
ciscoasa(config)# interface gi0/0
```

**Step 2**
Enable Layer 2 SGT Imposition and enter cts manual interface configuration mode.
```
ccts manual
```
Example:
```
ciscoasa(config-if)# cts manual
```

**Step 3**
Enable propagation of a security group tag on an interface. Propagation is enabled by default.
```
propagate sgt
```
Example:
```
ciscoasa(config-if-cts-manual)# propagate sgt
```

**Step 4**
Apply a policy to a manually configured CTS link.
```
policy static sgt sgt_number [trusted]
```
Example:
```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```
The `static` keyword specifies an SGT policy to incoming traffic on the link.
The `sgt sgt_number` keyword-argument pair specifies the SGT number to apply to incoming traffic from the peer. Valid values are from 2-65519.
The `trusted` keyword indicates that ingress traffic on the interface with the SGT specified in the command should not have its SGT overwritten. Untrusted is the default.

---

**Examples**
The following example enables an interface for Layer 2 SGT imposition and defines whether or not the interface is trusted:
```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
```
```
ciscoasa(config-if-cts-manual)# propagate sgt
```
```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

---

**Configure IP-SGT Bindings Manually**

To configure IP-SGT bindings manually, perform the following steps:

**Procedure**

**Step 1**
Configure IP-SGT bindings manually.
```
cts role-based sgt-map [IPv4_addr | IPv6_addr] sgt sgt_value
```
Example:
```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```
The `sgt sgt_value` keyword-argument pair specifies the SGT number. Valid values are from 2-65519.
Troubleshooting Tips

Use the **packet-tracer** command to determine why a particular session was allowed or denied, which SGT value is being used (from the SGT in the packet, from the IP-SGT manager, or from the **policy static sgt** command configured on the interface), and which security group-based security policies were applied.

The following example displays output from the **packet-tracer** command to show security group tag mapping to an IP address:

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.
```

Use the **capture capture-name type inline-tag tag** command to capture only the Cisco CMD packets (EtherType 0x8909) with or without a specific SGT value.

The following example displays output from the **show capture** command for a specified SGT value:

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

Example for Cisco TrustSec

The following example shows how to configure the ASA to use Cisco TrustSec:

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
ccts server-group cts-server-list
// Configure SXP peers
ccts sxp enable
  ccts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
  security-group name hr-admin-sg-name
  group-object it-admin
object-group security objgrp-hr-servers
  security-group name hr-servers-sg-name
  access-list hr-acl permit ip object-group-security objgrp-hr-admin any
  object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
```

Example for Cisco TrustSec

The following example shows how to configure the ASA to use Cisco TrustSec:

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
ccts server-group cts-server-list
// Configure SXP peers
ccts sxp enable
  ccts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
  security-group name hr-admin-sg-name
  group-object it-admin
object-group security objgrp-hr-servers
  security-group name hr-servers-sg-name
  access-list hr-acl permit ip object-group-security objgrp-hr-admin any
  object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
```
AnyConnect VPN Support for Cisco TrustSec

ASA Version 9.3(1) fully supports security group tagging of VPN sessions. A Security Group Tag (SGT) can be assigned to a VPN session using an external AAA server, or by configuration of the local user database. This tag can then be propagated through the Cisco TrustSec system over Layer 2 Ethernet. Security group tags are useful on group policies and for local users when the AAA server cannot provide an SGT.

If there is no SGT in the attributes from the AAA server to assign to a VPN user, then the ASA uses the SGT in the default group policy. If there is no SGT in the group policy, then tag 0x0 is assigned.

Typical Steps for a Remote User Connecting to a Server

1. A user connects to the ASA.
2. The ASA requests AAA information from the ISE, which may include an SGT. The ASA also assigns an IP address for the user’s tunneled traffic.
3. The ASA uses AAA information to authenticate and creates a tunnel.
4. The ASA uses the SGT from AAA information and the assigned IP address to add an SGT in the Layer 2 header.
5. Packets that include the SGT are passed to the next peer device in the Cisco TrustSec network.

Add an SGT to Local Users and Groups

To configure an SGT attribute on the LOCAL user database and in a group policy, perform the following steps:

Procedure

Step 1 Enter group-policy configuration mode.

```
group-policy name
```

Example:

```
ciscoasa(config)# group policy Grpolicy1
```

Step 2 Configure SGT attributes on the named group policy’s or LOCAL username’s attribute set.

```
security-group-tag value sgt
```

Example:

```
ciscoasa(config-group-policy)# security-group-tag value 101
```
The default form of this command is `security-group-tag none`, which means that there is no security group tag in this attribute set. Use the `no security-group-tag value sgt` command to return the configuration to the default.

## Monitoring Cisco TrustSec

See the following commands for monitoring Cisco TrustSec:

- **show running-config cts**
  Shows the configured default values for the Cisco TrustSec infrastructure and the SXP commands.

- **show running-config [all] cts role-based [sgt-map]**
  This command shows the user-defined IP-SGT binding table entries.

- **show cts xsp connections**
  This command shows the SXP connections on the ASA for a particular user context when multiple context mode is used.

- **show conn security-group**
  Shows data for all SXP connections.

- **show cts environment-data**
  Shows the Cisco TrustSec environment information contained in the security group table on the ASA.

- **show cts sgt-map**
  Shows the IP address-security group table manager entries in the control path.

- **show asp table cts sgt-map**
  This command shows the IP address-security group table mapping entries from the IP address-security group table mapping database maintained in the datapath.

- **show cts pac**
### Table 33-6  History for Cisco TrustSec

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco TrustSec</td>
<td>9.0(1)</td>
<td>Cisco TrustSec provides access control that builds on an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec feature, enforcement devices use a combination of user attributes and endpoint 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 use Cisco TrustSec for other types of security group-based policies, such as application inspection; for example, you can configure a class map that includes an access policy based on a security group. We introduced or modified the following commands: access-list extended, cts sxp enable, cts server-group, cts sxp default, cts sxp retry period, cts sxp reconciliation period, cts sxp connection peer, cts import-pac, cts refresh environment-data, object-group security, security-group, show running-config cts, show running-config object-group, clear configure cts, clear configure object-group, show cts pac, show cts environment-data, show cts environment-data sg-table, show cts sxp connections, show object-group, show configure security-group, clear cts environment-data, debug cts, and packet-tracer.</td>
</tr>
<tr>
<td>Layer 2 Security Group Tag Imposition</td>
<td>9.3(1)</td>
<td>You can now use security group tagging combined with Ethernet tagging to enforce policies. SGT plus Ethernet Tagging, also called Layer 2 SGT Imposition, enables the ASA to send and receive security group tags on Ethernet interfaces using Cisco proprietary Ethernet framing (EtherType 0x8909), which allows the insertion of source security group tags into plain-text Ethernet frames. We introduced or modified the following commands: cts manual, policy static sgt, propagate sgt, cts role-based sgt-map, show cts sgt-map, packet-tracer, capture, show capture, show asp drop, show asp table classify, show running-config all, clear configure all, and write memory.</td>
</tr>
</tbody>
</table>
Digital Certificates

This chapter describes how to configure digital certificates.

- About Digital Certificates, page 34-1
- Guidelines for Digital Certificates, page 34-9
- Monitoring Digital Certificates, page 34-40
- History for Certificate Management, page 34-42

About Digital Certificates

Digital certificates provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. CAs are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security.

For authentication using digital certificates, at least one identity certificate and its issuing CA certificate must exist on an ASA. This configuration allows multiple identities, roots, and certificate hierarchies. The ASA evaluates third-party certificates against CRLs, also called authority revocation lists, all the way from the identity certificate up the chain of subordinate certificate authorities.

Descriptions of several different types of available digital certificates follow:

- A CA certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.
- CAs also issue identity certificates, which are certificates for specific systems or hosts.
- Code signer certificates are special certificates that are used to create digital signatures to sign code, with the signed code itself revealing the certificate origin.

The local CA integrates an independent certificate authority feature on the ASA, deploys certificates, and provides secure revocation checking of issued certificates. The local CA provides a secure, configurable, in-house authority for certificate authentication with user enrollment through a website login page.

Note

CA certificates and identity certificates apply to both site-to-site VPN connections and remote access VPN connections. Procedures in this document refer to remote access VPN use in the ASDM GUI.
Digital certificates provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. CAs are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security.

For authentication using digital certificates, at least one identity certificate and its issuing CA certificate must exist on an ASA. This configuration allows multiple identities, roots, and certificate hierarchies. Descriptions of several different types of available digital certificates follow:

- A CA certificate is used to sign other certificates. It is self-signed and called a root certificate.
- A certificate that is issued by another CA certificate is called a subordinate certificate.

CAs are responsible for managing certificate requests and issuing digital certificates. A digital certificate includes information that identifies a user or device, such as a name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. A CA can be a trusted third party, such as VeriSign, or a private (in-house) CA that you establish within your organization.

For an example of a scenario that includes certificate configuration and load balancing, see the following URL: https://supportforums.cisco.com/docs/DOC-5964.

**Public Key Cryptography**

Digital signatures, enabled by public key cryptography, provide a way to authenticate devices and users. In public key cryptography, such as the RSA encryption system, each user has a key pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other.

In simple terms, a signature is formed when data is encrypted with a private key. The signature is attached to the data and sent to the receiver. The receiver applies the public key of the sender to the data. If the signature sent with the data matches the result of applying the public key to the data, the validity of the message is established.

This process relies on the receiver having a copy of the public key of the sender and a high degree of certainty that this key belongs to the sender, not to someone pretending to be the sender.

Obtaining the public key of a sender is normally handled externally or through an operation performed at installation. For example, most web browsers are configured with the root certificates of several CAs by default. For VPN, the IKE protocol, a component of IPsec, can use digital signatures to authenticate peer devices before setting up security associations.

**Certificate Scalability**

Without digital certificates, you must manually configure each IPsec peer for each peer with which it communicates; as a result, each new peer that you add to a network would require a configuration change on each peer with which it needs to communicate securely.

When you use digital certificates, each peer is enrolled with a CA. When two peers try to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, you enroll that peer with a CA and none of the other peers need modification. When the new peer attempts an IPsec connection, certificates are automatically exchanged and the peer can be authenticated.
With a CA, a peer authenticates itself to the remote peer by sending a certificate to the remote peer and performing some public key cryptography. Each peer sends its unique certificate, which was issued by the CA. This process works because each certificate encapsulates the public key for the associated peer, each certificate is authenticated by the CA, and all participating peers recognize the CA as an authenticating authority. The process is called IKE with an RSA signature.

The peer can continue sending its certificate for multiple IPsec sessions, and to multiple IPsec peers, until the certificate expires. When its certificate expires, the peer administrator must obtain a new one from the CA.

CAs can also revoke certificates for peers that no longer participate in IPsec. Revoked certificates are not recognized as valid by other peers. Revoked certificates are listed in a CRL, which each peer may check before accepting a certificate from another peer.

Some CAs have an RA as part of their implementation. An RA is a server that acts as a proxy for the CA, so that CA functions can continue when the CA is unavailable.

### Key Pairs

Key pairs are RSA keys, which have the following characteristics:

- RSA keys can be used for SSH or SSL.
- SCEP enrollment supports the certification of RSA keys.
- For the purposes of generating keys, the maximum key modulus for RSA keys is 2048 bits. The default size is 1024. Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause a high CPU usage on the ASA and rejected clientless logins.
- For signature operations, the supported maximum key size is 4096 bits. We recommend using a key size of at least 2048.
- You can generate a general purpose RSA key pair, used for both signing and encryption, or you can generate separate RSA key pairs for each purpose. Separate signing and encryption keys help to reduce exposure of the keys, because SSL uses a key for encryption but not signing. However, IKE uses a key for signing but not encryption. By using separate keys for each, exposure of the keys is minimized.

### Trustpoints

Trustpoints let you manage and track CAs and certificates. A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CA-specific configuration parameters, and an association with one, enrolled identity certificate.

After you have defined a trustpoint, you can reference it by name in commands requiring that you specify a CA. You can configure many trustpoints.

*Note*

If the Cisco ASA has multiple trustpoints that share the same CA, only one of these trustpoints sharing the CA can be used to validate user certificates. To control which trustpoint sharing a CA is used for validation of user certificates issued by that CA, use the `support-user-cert-validation` command.

For automatic enrollment, a trustpoint must be configured with an enrollment URL, and the CA that the trustpoint represents must be available on the network and must support SCEP.
You can export and import the keypair and issued certificates associated with a trustpoint in PKCS12 format. This format is useful to manually duplicate a trustpoint configuration on a different ASA.

**Certificate Enrollment**

The ASA needs a CA certificate for each trustpoint and one or two certificates for itself, depending upon the configuration of the keys used by the trustpoint. If the trustpoint uses separate RSA keys for signing and encryption, the ASA needs two certificates, one for each purpose. In other key configurations, only one certificate is needed.

The ASA supports automatic enrollment with SCEP and with manual enrollment, which lets you paste a base-64-encoded certificate directly into the terminal. For site-to-site VPNs, you must enroll each ASA. For remote access VPNs, you must enroll each ASA and each remote access VPN client.

**Proxy for SCEP Requests**

The ASA can proxy SCEP requests between AnyConnect and a third-party CA. The CA only needs to be accessible to the ASA if it is acting as the proxy. For the ASA to provide this service, the user must authenticate using any of the methods supported by AAA before the ASA sends an enrollment request. You can also use host scan and dynamic access policies to enforce rules of eligibility to enroll.

The ASA supports this feature only with an AnyConnect SSL or IKEv2 VPN session. It supports all SCEP-compliant CAs, including Cisco IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA.

Clientless (browser-based) access does not support SCEP proxy, although WebLaunch—clientless-initiated AnyConnect—does support it.

The ASA does not support polling for certificates.

The ASA supports load balancing for this feature.

**Revocation Checking**

When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a certificate before this time period expires; for example, because of security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the ASA to check that the CA has not revoked a certificate each time that it uses the certificate for authentication.

When you enable revocation checking, the ASA checks certificate revocation status during the PKI certificate validation process, which can use either CRL checking, OCSP, or both. OCSP is only used when the first method returns an error (for example, indicating that the server is unavailable).

With CRL checking, the ASA retrieves, parses, and caches CRLs, which provide a complete list of revoked (and unrevoked) certificates with their certificate serial numbers. The ASA evaluates certificates according to CRLs, also called authority revocation lists, from the identity certificate up the chain of subordinate certificate authorities.

OCSP offers a more scalable method of checking revocation status in that it localizes certificate status through a validation authority, which it queries for status of a specific certificate.
Supported CA Servers

The ASA supports the following CA servers:

Cisco IOS CS, ASA Local CA, and third-party X.509 compliant CA vendors including, but not limited to:

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRLs

CRLs provide the ASA with one way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. CRL configuration is part of configuration of a trustpoint. You can configure the ASA to make CRL checks mandatory when authenticating a certificate by using the `revocation-check crl` command. You can also make the CRL check optional by using the `revocation-check crl none` command, which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

The ASA can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a configurable amount of time for each trustpoint.

When the ASA has cached a CRL for longer than the amount of time it is configured to cache CRLs, the ASA considers the CRL too old to be reliable, or “stale.” The ASA tries to retrieve a newer version of the CRL the next time that a certificate authentication requires a check of the stale CRL.

The ASA caches CRLs for an amount of time determined by the following two factors:

- The number of minutes specified with the `cache-time` command. The default value is 60 minutes.
- The NextUpdate field in the CRLs retrieved, which may be absent from CRLs. You control whether the ASA requires and uses the NextUpdate field with the `enforcenextupdate` command.

The ASA uses these two factors in the following ways:

- If the NextUpdate field is not required, the ASA marks CRLs as stale after the length of time defined by the `cache-time` command.
- If the NextUpdate field is required, the ASA marks CRLs as stale at the sooner of the two times specified by the `cache-time` command and the NextUpdate field. For example, if the `cache-time` command is set to 100 minutes and the NextUpdate field specifies that the next update is 70 minutes away, the ASA marks CRLs as stale in 70 minutes.

If the ASA has insufficient memory to store all CRLs cached for a given trustpoint, it deletes the least recently used CRL to make room for a newly retrieved CRL.
OCSP

OCSP provides the ASA with a way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. OCSP configuration is part of trustpoint configuration.

OCSP localizes certificate status on a validation authority (an OCSP server, also called the responder) which the ASA queries for the status of a specific certificate. This method provides better scalability and more up-to-date revocation status than does CRL checking, and helps organizations with large PKI installations deploy and expand secure networks.

Note

The ASA allows a five-second time skew for OCSP responses.

You can configure the ASA to make OCSP checks mandatory when authenticating a certificate by using the `revocation-check ocsp` command. You can also make the OCSP check optional by using the `revocation-check ocsp none` command, which allows the certificate authentication to succeed when the validation authority is unavailable to provide updated OCSP data.

OCSP provides three ways to define the OCSP server URL. The ASA uses these servers in the following order:

1. The OCSP URL defined in a match certificate override rule by using the `match certificate` command).
2. The OCSP URL configured by using the `ocsp url` command.
3. The AIA field of the client certificate.

Note

To configure a trustpoint to validate a self-signed OCSP responder certificate, you import the self-signed responder certificate into its own trustpoint as a trusted CA certificate. Then you configure the `match certificate` command in the client certificate validating trustpoint to use the trustpoint that includes the self-signed OCSP responder certificate to validate the responder certificate. Use the same procedure for configuring validating responder certificates external to the validation path of the client certificate.

The OCSP server (responder) certificate usually signs the OCSP response. After receiving the response, the ASA tries to verify the responder certificate. The CA normally sets the lifetime of the OCSP responder certificate to a relatively short period to minimize the chance of being compromised. The CA usually also includes an ocsp-no-check extension in the responder certificate, which indicates that this certificate does not need revocation status checking. However, if this extension is not present, the ASA tries to check revocation status using the same method specified in the trustpoint. If the responder certificate is not verifiable, revocation checks fail. To avoid this possibility, use the `revocation-check none` command to configure the responder certificate validating trustpoint, and use the `revocation-check ocsp` command to configure the client certificate.

The Local CA

The local CA performs the following tasks:

- Integrates basic certificate authority operation on the ASA.
- Deploys certificates.
- Provides secure revocation checking of issued certificates.
- Provides a certificate authority on the ASA for use with browser-based and client-based SSL VPN connections.
• Provides trusted digital certificates to users, without the need to rely on external certificate authorization.
• Provides a secure, in-house authority for certificate authentication and offers straightforward user enrollment by means of a website login.

Storage for Local CA Files

The ASA accesses and implements user information, issued certificates, and revocation lists using a local CA database. This database resides in local flash memory by default, or can be configured to reside on an external file system that is mounted and accessible to the ASA.

No limits exist on the number of users that can be stored in the local CA user database; however, if flash memory storage issues arise, syslogs are generated to alert the administrator to take action, and the local CA could be disabled until the storage issues are resolved. Flash memory can store a database with 3500 users or less; however, a database of more than 3500 users requires external storage.

The Local CA Server

After you configure a local CA server on the ASA, users can enroll for a certificate by logging into a website and entering a username and a one-time password that is provided by the local CA administrator to validate their eligibility for enrollment.

Figure 34-1 shows that the local CA server resides on the ASA and handles enrollment requests from website users and CRL inquiries coming from other certificate validating devices and ASAs. Local CA database and configuration files are maintained either on the ASA flash memory (default storage) or on a separate storage device.

Figure 34-1 The Local CA
Certificates and User Login Credentials

The following section describes the different methods of using certificates and user login credentials (username and password) for authentication and authorization. These methods apply to IPsec, AnyConnect, and Clientless SSL VPN.

In all cases, LDAP authorization does not use the password as a credential. RADIUS authorization uses either a common password for all users or the username as a password.

User Login Credentials

The default method for authentication and authorization uses the user login credentials.

- **Authentication**
  - Enabled by the authentication server group setting in the tunnel group (also called ASDM Connection Profile)
  - Uses the username and password as credentials

- **Authorization**
  - Enabled by the authorization server group setting in the tunnel group (also called ASDM Connection Profile)
  - Uses the username as a credential

Certificates

If user digital certificates are configured, the ASA first validates the certificate. It does not, however, use any of the DNs from certificates as a username for the authentication.

If both authentication and authorization are enabled, the ASA uses the user login credentials for both user authentication and authorization.

- **Authentication**
  - Enabled by the authentication server group setting
  - Uses the username and password as credentials

- **Authorization**
  - Enabled by the authorization server group setting
  - Uses the username as a credential

If authentication is disabled and authorization is enabled, the ASA uses the primary DN field for authorization.

- **Authentication**
  - DISABLED (set to None) by the authentication server group setting
  - No credentials used

- **Authorization**
  - Enabled by the authorization server group setting
  - Uses the username value of the certificate primary DN field as a credential
Note
If the primary DN field is not present in the certificate, the ASA uses the secondary DN field value as the username for the authorization request.

For example, consider a user certificate that includes the following Subject DN fields and values:

\[Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com\]

If the Primary DN = EA (E-mail Address) and the Secondary DN = CN (Common Name), then the username used in the authorization request would be anyuser@example.com.

Guidelines for Digital Certificates

This section includes guidelines and limitations that you should check before configuring digital certificates.

Context Mode Guidelines
- Supported in single context mode only for third-party CAs.

Failover Guidelines
- Does not support replicating sessions in Stateful Failover.
- Does not support failover for local CAs.

IPv6 Guidelines
Does not support IPv6.

Local CA Certificates
- Make sure that the ASA is configured correctly to support certificates. An incorrectly configured ASA can cause enrollment to fail or request a certificate that includes inaccurate information.
- Make sure that the hostname and domain name of the ASA are configured correctly. To view the currently configured hostname and domain name, enter the `show running-config` command.
- Make sure that the ASA clock is set accurately before configuring the CA. Certificates have a date and time that they become valid and expire. When the ASA enrolls with a CA and obtains a certificate, the ASA checks that the current time is within the valid range for the certificate. If it is outside that range, enrollment fails.
- Thirty days before the local CA certificate expires, a rollover replacement certificate is generated, and a syslog message informs the administrator that it is time for local CA rollover. The new local CA certificate must be imported onto all necessary devices before the current certificate expires. If the administrator does not respond by installing the rollover certificate as the new local CA certificate, validations may fail.
- The local CA certificate rolls over automatically after expiration using the same keypair. The rollover certificate is available for export in base 64 format.

The following example shows a base 64 encoded local CA certificate:

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaaCCF0IgEhc=MIIXOjCCF1EGCSqGSIb3DQEHAaaCCF0IgEhc=MIIXOjCCF1EGCSqGSIb3DQEHBqCCFye=cwghcjaqEAMIXHA
YJKoZIhvcNAQc=MBMoGCSqGSIb3DQEJbMDQgMA0GCSqGSIb3DQEJbMDQgMA0GCSqGSIb3DQEJbMDQgMA0GCSqGSIb3DQEJbMDQgMA0GCSqGSIb3DQEJbMDQgMA

0Iqph4SxJoyTqCAQgAgwb3v4bFy=+GG2dJnB40LpJm+1G3S

```

Cisco ASA Series General Operations CLI Configuration Guide

34-9
Guidelines for Digital Certificates

PrzoGlJ8BFq3Pa1jBGhAzzuSmE1m3jJ/2dqI3Atr0lG9nIsRh9Y39feBgwz4fEabHG7/Vanb+fs8d5n10iJjDYY
bP6tvrb2y0VZ6aK6fV10b2AfcCr6Pbwc9U8Z/aF3BCyMz2n2xPJxXva94CaYrqyotZdAkSYA5KwScyEcdqmu
BeGDKnTkmfgy0XM+fG5rb3gAXy1GkjyFI5Bm9Do6RUR0oG1DSrQKeg/hj...

END OF CERTIFICATE

SCEP Proxy Support

- AnyConnect Secure Mobility Client 3.0 or later must be running at the endpoint.
- The authentication method, configured in the connection profile for your group policy, must be set to use both AAA and certificate authentication.
- An SSL port must be open for IKEv2 VPN connections.
- The CA must be in auto-grant mode.

Local CA Certificate Database

To maintain the local CA certificate database, make sure that you save the certificate database file, LOCAL-CA-SERVER.cdb, with the write memory command each time that a change to the database occurs. The local CA certificate database includes the following files:

- The LOCAL-CA-SERVER.p12 file is the archive of the local CA certificate and keypair that is generated when the local CA server is initially enabled.
- The LOCAL-CA-SERVER.crl file is the actual CRL.
- The LOCAL-CA-SERVER.ser file keeps track of the issued certificate serial numbers.

Additional Guidelines

- For ASAs that are configured as CA servers or clients, limit the validity period of the certificate to less than the recommended end date of 03:14:08 UTC, January 19, 2038. This guideline also applies to imported certificates from third-party vendors.
- You cannot configure the local CA when failover is enabled. You can only configure the local CA server for standalone ASAs without failover. For more information, see CSCty43366.
- When a certificate enrollment is completed, the ASA stores a PKCS12 file containing the user's keypair and certificate chain, which requires about 2 KB of flash memory or disk space per enrollment. The actual amount of disk space depends on the configured RSA key size and certificate fields. Keep this guideline in mind when adding a large number of pending certificate enrollments on an ASA with a limited amount of available flash memory, because these PKCS12 files are stored in flash memory for the duration of the configured enrollment retrieval timeout. We recommend using a key size of at least 2048.
- The lifetime ca-certificate command takes effect when the local CA server certificate is first generated (that is, when you initially configure the local CA server and issue the no shutdown command). When the CA certificate expires, the configured lifetime value is used to generate the new CA certificate. You cannot change the lifetime value for existing CA certificates.
- You should configure the ASA to use an identity certificate to protect ASDM traffic and HTTPS traffic to the management interface. Identity certificates that are automatically generated with SCEP are regenerated after each reboot, so make sure that you manually install your own identity certificates. For an example of this procedure that applies only to SSL, see the following URL: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
The ASA and the AnyConnect clients can only validate certificates in which the X520SerialNumber field (the serial number in the Subject Name) is in PrintableString format. If the serial number format uses encoding such as UTF8, the certificate authorization will fail.

Use only valid characters and values for certificate parameters when you import them on the ASA.

To use a wildcard (*) symbol, make sure that you use encoding on the CA server that allows this character in the string value. Although RFC 5280 recommends using either a UTF8String or PrintableString, you should use UTF8String because PrintableString does not recognize the wildcard as a valid character. The ASA rejects the imported certificate if an invalid character or value is found during the import. For example:

```
ERROR: Failed to parse or verify imported certificate
ciscoasa(config)# Read
162*H-ytes as CA certificate: 0U0= \Ivr^phÖV°3éq0
CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../../source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
mm.
CERT-C: E ../../source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795): crypto_certc_pkcs7_extract_certs_and_crls
failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

### Configure Key Pairs

To create or remove key pairs, perform the following steps:

**Procedure**

**Step 1** Generate one, general-purpose RSA key pair.

```cli
crypto key generate rsa
```

Example:

```
ciscoasa/contexta(config)# crypto key generate rsa
```

The default key modulus is 1024. To specify other modulus sizes, use the `modulus` keyword.

**Note** Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause high CPU usage on the ASA and rejected clientless logins.

**Step 2** (Optional) Assign a label to each key pair.

```cli
crypto key generate rsa label key-pair-label
```

Example:

```
ciscoasa/contexta(config)# crypto key generate rsa label exchange
```

The label is referenced by the trustpoint that uses the key pair. If you do not assign a label, the key pair is automatically labeled, `Default-RSA-Key`.

**Step 3** Verify key pairs that you have generated.

```cli
show crypto key name of key
```

Example:
Step 4  Save the key pair that you have generated.
        write memory

        Example:
        ciscoasa(config)# write memory

Step 5  If necessary, remove existing key pairs so that you can generate new ones.
        crypto key zeroize rsa

        Example:
        ciscoasa(config)# crypto key zeroize rsa

Step 6  (Optional) Archive the local CA server certificate and keypair.
        copy

        Example:
        ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/

        This command copies the local CA server certificate and keypair and all files from the ASA using either
        FTP or TFTP.

        **Note**  Make sure that you back up all local CA files as often as possible.

        **Examples**
        The following example shows how to remove key pairs:
        ciscoasa(config)# crypto key zeroize rsa
        WARNING: All RSA keys will be removed.
        WARNING: All device certs issued using these keys will also be removed.
        Do you really want to remove these keys? [yes/no]  y

**Configure Trustpoints**

To configure a trustpoint, perform the following steps:

**Procedure**

Step 1  Create a trustpoint that corresponds to the CA from which the ASA needs to receive a certificate.
        crypto ca trustpoint trustpoint-name

        Example:
        ciscoasa/contexta(config)# crypto ca trustpoint Main

        You enter the crypto ca trustpoint configuration mode, which controls CA-specific trustpoint parameters
        that you may configure starting in Step 3.
Note When you try to connect, a warning occurs to indicate that the trustpoint does not contain an ID certificate when an attempt is made to retrieve the ID certificate from the trustpoint.

Step 2 Choose one of the following options:

- Request automatic enrollment using SCEP with the specified trustpoint and configures the enrollment URL.
  
  **enrollment url url**
  
  Example:
  
  ```
ciscoasa/contexta(config-ca-trustpoint)# enrollment url http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

- Request manual enrollment with the specified trustpoint by pasting the certificate received from the CA into the terminal.
  
  **enrollment terminal**
  
  Example:
  
  ```
ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
  ```

Step 3 Specify the available CRL configuration options.

  **revocation-check crl none**
  
  Example:
  
  ```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl none
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
nciscoasa/contexta(config-ca-trustpoint)# revocation-check none
  ```

Note To enable either required or optional CRL checking, make sure that you configure the trustpoint for CRL management after obtaining certificates.

Step 4 Enter crl configuration mode.

  **crl configure**
  
  Example:
  
  ```
ciscoasa/contexta(config-ca-trustpoint)# crl configure
  ```

Step 5 During enrollment, ask the CA to include the specified e-mail address in the Subject Alternative Name extension of the certificate.

  **email address**
  
  Example:
  
  ```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
  ```

Step 6 (Optional) Specify a retry period in minutes, and applies only to SCEP enrollment.

  **enrollment retry period**
  
  Example:
  
  ```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
  ```
Step 7  (Optional) Specify a maximum number of permitted retries, and applies only to SCEP enrollment.

```plaintext
enrollment retry count
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

Step 8  During enrollment, ask the CA to include the specified fully qualified domain name in the Subject Alternative Name extension of the certificate.

```plaintext
fqdn fqdn
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

Step 9  During enrollment, ask the CA to include the IP address of the ASA in the certificate.

```plaintext
ip-address ip-address
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

Step 10 Specify the key pair whose public key is to be certified.

```plaintext
keypair name
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

Step 11  Configure OCSP URL overrides and trustpoints to use for validating OCSP responder certificates.

```plaintext
match certificate map-name override ocsp
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

Step 12  Disable the nonce extension on an OCSP request. The nonce extension cryptographically binds requests with responses to avoid replay attacks.

```plaintext
ocsp disable-nonce
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

Step 13  Configure an OCSP server for the ASA to use to check all certificates associated with a trustpoint rather than the server specified in the AIA extension of the client certificate.

```plaintext
ocsp url
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

Step 14  Specify a challenge phrase that is registered with the CA during enrollment. The CA usually uses this phrase to authenticate a subsequent revocation request.

```plaintext
password string
```

Example:
```bash
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```
Step 15 Set one or more methods for revocation checking: CRL, OCSP, and none.
```
revocation check
```
Example:
```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

Step 16 During enrollment, ask the CA to include the specified subject DN in the certificate. If a DN string includes a comma, enclose the value string within double quotes (for example, O="Company, Inc.").
```
subject-name X.500 name
```
Example:
```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

Step 17 During enrollment, ask the CA to include the ASA serial number in the certificate.
```
serial-number
```
Example:
```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

Step 18 Save the running configuration.
```
write memory
```
Example:
```
ciscoasa/contexta(config)# write memory
```

---

**Configure CRLs for a Trustpoint**

To use mandatory or optional CRL checking during certificate authentication, you must configure CRLs for each trustpoint. To configure CRLs for a trustpoint, perform the following steps:

**Procedure**

Step 1 Enter crypto ca trustpoint configuration mode for the trustpoint whose CRL configuration you want to modify.
```
crypto ca trustpoint trustpoint-name
```
Example:
```
ciscoasa (config)# crypto ca trustpoint Main
```

**Note** Make sure that you have enabled CRLs before entering this command. In addition, the CRL must be available for authentication to succeed.

Step 2 Enter crl configuration mode for the current trustpoint.
```
crl configure
```
Example:
ciscoasa(config-ca-trustpoint)# crl configure

**Tip**  To set all CRL configuration parameters to default values, use the `default` command. At any time during CRL configuration, reenter this command to restart the procedure.

**Step 3**  Choose one of the following to configure retrieval policy:

- CRLs are retrieved only from the CRL distribution points that are specified in authenticated certificates.
  
  `policy cdp`

  Example:
  
  `ciscoasa(config-ca-crl)# policy cdp`

  **Note**  SCEP retrieval is not supported by distribution points specified in certificates.

  To continue, go to Step 5.

- CRLs are retrieved only from URLs that you configure.
  
  `policy static`

  Example:
  
  `ciscoasa(config-ca-crl)# policy static`

  To continue, go to Step 4.

- CRLs are retrieved from CRL distribution points specified in authenticated certificates and from URLs that you configure.
  
  `policy both`

  Example:
  
  `ciscoasa(config-ca-crl)# policy both`

  To continue, go to Step 4.

**Step 4**  If you used the `static` or `both` keywords when you configured the CRL policy, you must configure URLs for CRL retrieval. You can enter up to five URLs, ranked 1 through 5. The `n` argument is the rank assigned to the URL.

`url n url`

Example:

`ciscoasa (config-ca-crl)# url 2 http://www.example.com`

To remove a URL, use the `no url n` command.

**Step 5**  Specify HTTP, LDAP, or SCEP as the CRL retrieval method.

`protocol http | idap | scep`

Example:

`ciscoasa(config-ca-crl)# protocol http`
Step 6  Configure how long the ASA caches CRLs for the current trustpoint. The refresh-time argument is the number of minutes that the ASA waits before considering a CRL stale.

    cache-time refresh-time

Example:

ciscoasa(config-ca-crl)# cache-time 420

Step 7  Choose one of the following:

- Require the NextUpdate field to be present in CRLs. This is the default setting.

    enforcenextupdate

Example:

ciscoasa(config-ca-crl)# enforcenextupdate

- Allow the NextUpdate field to be absent in CRLs.

    no enforcenextupdate

Example:

ciscoasa(config-ca-crl)# no enforcenextupdate

Step 8  Identify the LDAP server to the ASA if LDAP is specified as the retrieval protocol. You can specify the server by DNS hostname or by IP address. You can also provide a port number if the server listens for LDAP queries on a port other than the default of 389.

    ldap-defaults server

Example:

ciscoasa(config-ca-crl)# ldap-defaults ldap1

Note  If you use a hostname instead of an IP address to specify the LDAP server, make sure that you have configured the ASA to use DNS.

Step 9  Allow CRL retrieval if the LDAP server requires credentials.

    ldap-dn admin-DN password

Example:

ciscoasa(config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ

Step 10 Retrieve the current CRL from the CA represented by the specified trustpoint and test the CRL configuration for the current trustpoint.

    crypto ca crl request trustpoint

Example:

ciscoasa(config-ca-crl)# crypto ca crl request Main

Step 11 Save the running configuration.

    write memory

Example:

ciscoasa(config)# write memory
Export or Import a Trustpoint Configuration

To export a trustpoint configuration, perform the following steps:

**Procedure**

**Step 1**
Export a trustpoint configuration with all associated keys and certificates in PKCS12 format.

```
crypto ca export trustpoint
```

Example:

```
ciscoasa(config)# crypto ca export Main
```

The ASA displays the PKCS12 data in the terminal. You can copy the data. The trustpoint data is password protected; however, if you save the trustpoint data in a file, make sure that the file is in a secure location.

**Examples**

The following example exports PKCS12 data for the trustpoint Main with the passphrase Wh0zits:

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits
```

Exported pkcs12 follows:

```
{ PKCS12 data omitted }

---End - This line not part of the pkcs12---
```

To import a trustpoint configuration, perform the following steps:

**Step 1**
Import keypairs and issued certificates that are associated with a trustpoint configuration.

```
crypto ca import trustpoint pkcs12
```

Example:

```
ciscoasa(config)# crypto ca import Main pkcs12
```

The ASA prompts you to paste the text into the terminal in base 64 format. The key pair imported with the trustpoint is assigned a label that matches the name of the trustpoint that you create.

**Note**

If an ASA has trustpoints that share the same CA, you can use only one of the trustpoints that share the CA to validate user certificates. To control which trustpoint that shares a CA is used for validation of user certificates issued by that CA, use the `support-user-cert-validation` keyword.
Examples

The following example manually imports PKCS12 data to the trustpoint Main with the passphrase Wh0zits:

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits
```

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully

The following example manually imports a certificate for the trustpoint Main:

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com
```

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported

Configure CA Certificate Map Rules

You can configure rules based on the Issuer and Subject fields of a certificate. Using the rules you create, you can map IPsec peer certificates to tunnel groups with the `tunnel-group-map` command. The ASA supports one CA certificate map, which can include many rules.

To configure a CA certificate map rule, perform the following steps:

**Procedure**

**Step 1**
Enter CA certificate map configuration mode for the rule you want to configure and specify the rule index number.

```
crypto ca certificate map sequence-number
```

Example:
```
ciscoasa(config)# crypto ca certificate map 1
```

**Step 2**
Specify the distinguished name of all issued certificates, which is also the subject-name DN of the self-signed CA certificate.

```
issuer-name DN-string
```

Example:
```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
```

Use commas to separate attribute-value pairs. Insert quotation marks around any value that includes a comma. An issuer-name must be less than 500 alphanumeric characters. The default issuer-name is `cn=hostname.domain-name`.

**Step 3**
Specify tests that the ASA can apply to values found in the Subject field of certificates.

```
subject-name attr tag eq | co | ne | nc string
```

Example:

ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert

The tests can apply to specific attributes or to the entire field. You can configure many tests per rule, and all the tests you specify with these commands must be true for a rule to match a certificate. The following are valid operators:

- **eq**—The field or attribute must be identical to the value given.
- **ne**—The field or attribute cannot be identical to the value given.
- **co**—Part or all of the field or attribute must match the value given.
- **nc**—No part of the field or attribute can match the value given.

**Step 4** Save the running configuration.

`write memory`

Example:

ciscoasa(config)# write memory

---

## Obtain Certificates Manually

This section describes how to obtain certificates manually.

**Before You Begin**

You must have already obtained a base-64 encoded CA certificate from the CA represented by the trustpoint.

To obtain certificates manually, perform the following steps:

**Procedure**

**Step 1** Import the CA certificate for the configured trustpoint.

`crypto ca authenticate trustpoint`

Example:

ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTMNbGqwhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8iZY6EOTS6rKu7N76jWf5E4gtkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported

Whether a trustpoint requires that you manually obtain certificates is determined by the use of the `enrollment terminal` command when you configure the trustpoint.
Step 2
Enroll the ASA with the trustpoint.

crypto ca enroll trustpoint

Example:
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+Rb10Ymvt8g6hn8Trd0GqjjVLT

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: n

This command generates a certificate for signing data and depending on the type of keys that you have configured, for encrypting data. If you use separate RSA keys for signing and encryption, the crypto ca enroll command displays two certificate requests, one for each key. If you use general-purpose RSA keys for both signing and encryption, the crypto ca enroll command displays one certificate request.

To complete enrollment, obtain a certificate for all certificate requests generated by the crypto ca enroll command from the CA represented by the applicable trustpoint. Make sure that the certificate is in base-64 format.

Step 3
Import each certificate you receive from the CA and make sure that you paste the certificate to the terminal in base-64 format.

crypto ca import trustpoint certificate

Example:
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported

Step 4
Verify that the enrollment process was successful by displaying certificate details issued for the ASA and the CA certificate for the trustpoint.

show crypto ca server certificate

Example:
ciscoasa(config)# show crypto ca server certificate Main

Step 5
Save the running configuration.

write memory

Example:
Guidelines for Digital Certificates

Chapter 34      Digital Certificates

Guidelines for Digital Certificates

ciscoasa(config)# write memory

Step 6  Repeat these steps for each trustpoint that you configure for manual enrollment.

---

Obtain Certificates Automatically with SCEP

This section describes how to obtain certificates automatically using SCEP.

Before You Begin
You must have already obtained a base-64 encoded CA certificate from the CA represented by the trustpoint.

To obtain certificates automatically using SCEP, perform the following steps:

Procedure

Step 1  Obtain the CA certificate for the configured trustpoint.

crypto ca authenticate trustpoint

Example:
ciscoasa/contexta(config)# crypto ca authenticate Main

When you configure the trustpoint, use of the enrollment url command determines whether or not you must obtain certificates automatically via SCEP.

Step 2  Enroll the ASA with the trustpoint. This command retrieves a certificate for signing data and depending on the type of keys that you have configured, for encrypting data. Before entering this command, contact the CA administrator, who may need to authenticate the enrollment request manually before the CA grants certificates.

crypto ca enroll trustpoint

Example:
ciscoasa/contexta(config)# crypto ca enroll Main

If the ASA does not receive a certificate from the CA within one minute (the default) of sending a certificate request, it resends the certificate request. The ASA continues sending a certificate request each minute until a certificate is received.

If the fully qualified domain name configured for the trustpoint is not identical to the fully qualified domain name of the ASA, including the case of the characters, a warning appears. To resolve this issue, exit the enrollment process, make any necessary corrections, and reenter the crypto ca enroll command.

Note  If the ASA reboots after you have issued the crypto ca enroll command but before you have received the certificate, reenter the crypto ca enroll command and notify the CA administrator.

Step 3  Verify that the enrollment process was successful by displaying certificate details issued for the ASA and the CA certificate for the trustpoint.

show crypto ca server certificate

Example:
Cisco ASA Series General Operations CLI Configuration Guide

Chapter 34      Digital Certificates

Guidelines for Digital Certificates

ciscoasa/contexta(config)# show crypto ca server certificate Main

Step 4  Save the running configuration.
write memory
Example:
ciscoasa/contexta(config)# write memory

Configure Proxy Support for SCEP Requests

To configure the ASA to authenticate remote access endpoints using third-party CAs, perform the following steps:

Procedure

Step 1  Enter tunnel-group ipsec-attributes configuration mode.
tunnel-group name ipsec-attributes
Example:
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes

Step 2  Enable client services.
crypto ikev2 enable outside client-services port portnumber
Example:
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
The default port number is 443.

Note  This command is needed only if you support IKEv2.

Step 3  Enter tunnel-group general-attributes configuration mode.
tunnel-group name general-attributes
Example:
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes

Step 4  Enable SCEP enrollment for the tunnel group.
scep-enrollment enable
Example:
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this option.

Step 5  Enter group-policy attributes configuration mode.
group-policy name attributes
Example:
ciscoasa(config)# group-policy FirstGroup attributes

**Step 6** Enroll the SCEP CA for the group policy. Enter this command once per group policy to support a third-party digital certificate.

```plaintext
scep-forwarding-url value URL
```

Example:
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/

*URL* is the SCEP URL on the CA.

**Step 7** Supply a common, secondary password when a certificate is unavailable for WebLaunch support of the SCEP proxy.

```plaintext
secondary-pre-fill-username clientless hide use-common-password password
```

Example:
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide use-common-password secret

You must use the `hide` keyword to support the SCEP proxy.

For example, a certificate is not available to an endpoint requesting one. Once the endpoint has the certificate, AnyConnect disconnects, then reconnects to the ASA to qualify for a DAP policy that provides access to internal network resources.

**Step 8** Hide the secondary prefill username for AnyConnect VPN sessions.

```plaintext
secondary-pre-fill-username ssl-client hide use-common-password password
```

Example:
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide use-common-password secret

Despite the `ssl-client` keyword inherited from earlier releases, use this command to support AnyConnect sessions that use either IKEv2 or SSL.

You must use the `hide` keyword to support the SCEP proxy.

**Step 9** Supply the username when a certificate is unavailable.

```plaintext
secondary-username-from-certificate (use-entire-name | use-script | {primary_attr [secondary-attr]}) [no-certificate-fallback cisco-secure-desktop machine-unique-id]
```

Example:
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback cisco-secure-desktop machine-unique-id

---

**Enable the Local CA Server**

This section describes how to enable the local CA server.
Before You Begin

Before enabling the local CA server, you must first create a passphrase of at least seven characters to encode and archive a PKCS12 file that includes the local CA certificate and keypair to be generated. The passphrase unlocks the PKCS12 archive if the CA certificate or keypair is lost.

To enable the local CA server, perform the following steps:

Procedure

Step 1 Enter local ca server configuration mode.

```
crypto ca server
```

Example:
```
ciscoasa(config)# crypto ca server
```

Step 2 Enable the local CA server.

```
no shutdown
```

Example:
```
ciscoasa(config-ca-server)# no shutdown
```

This command generates the local CA server certificate, keypair and necessary database files, and archives the local CA server certificate and keypair in a PKCS12 file. You must enter an 8-65 alphanumeric password. After initial startup, you can disable the local CA without being prompted for the password.

Step 3 Save the configuration to make sure that the local CA certificate and keypair are not lost after a reboot occurs.

```
write memory
```

Example:
```
ciscoasa(config)# write memory
```

Examples

The following example enables the local CA server:
```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no shutdown
```

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver
Re-enter password: caserver

Keypair generation process begin. Please wait...

The following is sample output that shows local CA server configuration and status:
```
Certificate Server LOCAL-CA-SERVER:
  Status: enabled
  State: enabled
```
Configure the Local CA Server

To configure the local CA server, perform the following steps:

Procedure

**Step 1** Enter local ca server configuration mode.

```plaintext
crypto ca server
```

Example:

```
ciscoasa(config)# crypto ca server
```

**Step 2** Specify the SMTP from-address, a valid e-mail address that the local CA uses as a from address when sending e-mail messages that deliver one-time passwords (OTPs) for an enrollment invitation to users.

```plaintext
smtp from-address e-mail_address
```

Example:

```
ciscoasa(config-ca-server) # smtp from-address SecurityAdmin@example.com
```

**Step 3** (Optional) Specify the subject-name DN that is appended to each username on issued certificates.

```plaintext
subject-name-default dn
```

Example:

```
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc systems, c="US"
```

The subject-name DN and the username combine to form the DN in all user certificates that are issued by the local CA server. If you do not specify a subject-name DN, you must specify the exact subject name DN to be included in a user certificate each time that you add a user to the user database.

**Note** Make sure that you review all optional parameters carefully before you enable the configured local CA, because you cannot change issuer-name and keysize server values after you enable the local CA for the first time.

**Step 4** Create the self-signed certificate and associate it with the local CA on the ASA.

```plaintext
no shutdown
```

Example:

```
ciscoasa(config-ca-server)# no shutdown
```
The self-signed certificate key usage extension has key encryption, key signature, CRL signing, and certificate signing capabilities.

**Note** After the self-signed local CA certificate has been generated, to change any characteristics, you must delete the existing local CA server and completely recreate it.

The local CA server keeps track of user certificates, so the administrator can revoke or restore privileges as needed.

**Examples**

The following example shows how to configure the local CA server using the predefined default values for all required parameters:

```bash
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc Systems, c=US
```

**Customize the Local CA Server**

To configure a customized local CA server, perform the following steps:

**Procedure**

**Step 1** Enter local ca server configuration mode.

```bash
crypto ca server
```

Example:

```bash
ciscoasa(config)# crypto ca server
```

**Step 2** Specify parameters that do not have default values.

```bash
issuer-name DN-string
```

Example:

```bash
ciscoasa(config-ca-server)# issuer-name cn=xx5520,cn=30.132.0.25,ou=DevTest,ou=QA,o=ASC Systems
```

**Step 3** Customize the text that appears in the subject field of all e-mail messages sent from the local CA server.

```bash
smtp subject subject-line
```

Example:

```bash
ciscoasa(config-ca-server)# smtp subject Priority E-Mail: Enclosed Confidential Information is Required for Enrollment
```

**Step 4** Specify the e-mail address that is to be used as the From: field of all e-mail messages that are generated by the local CA server.

```bash
smtp from-address e-mail_address
```
Example:
```
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
```

### Step 5
Specify an optional subject-name DN to be appended to a username on issued certificates.

```
subject-name-default dn
```

Example:
```
ciscoasa(config-ca-server)# subject-name default cn=engineer, o=ASC Systems, c=US
```

The default subject-name DN becomes part of the username in all user certificates issued by the local CA server.

The allowed DN attribute keywords are as follows:

- **C** = Country
- **CN** = Common Name
- **EA** = E-mail Address
- **L** = Locality
- **O** = Organization Name
- **OU** = Organization Unit
- **ST** = State/Province
- **SN** = Surname
- **ST** = State/Province

----

**Note**
If you do not specify a subject-name-default to serve as a standard subject-name default, you must specify a DN each time that you add a user.

---

### Disable the Local CA Server

To disable the local CA server, perform the following steps:

#### Procedure

1. **Step 1**
   Enter local ca server configuration mode.
   
   ```
crypto ca server
   ```
   
   Example:
   ```
ciscoasa(config)# crypto ca server
   ```

2. **Step 2**
   Disable the local CA server.
   
   ```
shutdown
   ```
   
   Example:
   ```
ciscoasa(config-ca-server)# shutdown
   INFO: Local CA Server has been shutdown.
   ```
This command disables website enrollment, allows you to modify the local CA server configuration, and stores the current configuration and associated files. After initial startup, you can reenable the local CA without being prompted for the password.

**Delete the Local CA Server**

To delete an existing local CA server (either enabled or disabled), perform the following steps:

**Procedure**

**Step 1** Enter one of the following commands to remove an existing local CA server (either enabled or disabled):

- **no crypto ca server**
  - Example: `ciscoasa(config)# no crypto ca server`

- **clear configure crypto ca server**
  - Example: `ciscoasa(config)# clear config crypto ca server`

**Note** Deleting the local CA server removes the configuration from the ASA. After the configuration has been deleted, it is unrecoverable.

Make sure that you also delete the associated local CA server database and configuration files (that is, all files with the wildcard name, LOCAL-CA-SERVER.*).

**Configure the CA Certificate Lifetime**

To configure the local CA server certificate lifetime, perform the following steps:

**Procedure**

**Step 1** Enter local ca server configuration mode.

```
crypto ca server
```

- Example: `ciscoasa(config)# crypto ca server`

**Step 2** Determine the expiration date to be included in the certificate. The default lifetime of a local CA certificate is three years.

```
lifetime ca-certificate time
```

- Example:
Guidelines for Digital Certificates

Step 3  (Optional) Reset the local CA certificate lifetime to the default value of three years.

Example:

```
ciscoasa(config-ca-server)# no lifetime ca-certificate
```

The local CA server automatically generates a replacement CA certificate 30 days before it expires, which allows the replacement certificate to be exported and imported onto any other devices for certificate validation of user certificates that have been issued by the local CA certificate after the current local CA certificate has expired. The following pre-expiration syslog message is generated:

```
%ASA-1-717049: Local CA Server certificate is due to expire in days days and a replacement certificate is available for export.
```

**Note**  When notified of this automatic rollover, the administrator must make sure that the new local CA certificate is imported onto all required devices before it expires.

---

**Configure the User Certificate Lifetime**

To configure the user certificate lifetime, perform the following steps:

**Procedure**

**Step 1**  Enter local ca server configuration mode.

```
crypto ca server
```

Example:

```
ciscoasa(config)# crypto ca server
```

**Step 2**  Set the length of time that you want user certificates to remain valid.

```
lifetime certificate time
```

Example:

```
ciscoasa(config-ca-server)# lifetime certificate 60
```
Configure the CRL Lifetime

To configure the CRL lifetime, perform the following steps:

**Procedure**

**Step 1** Enter local ca server configuration mode.

```
crypto ca server
```

Example:
```
ciscoasa(config)# crypto ca server
```

**Step 2** Set the length of time that you want the CRL to remain valid.

```
lifetime crl time
```

Example:
```
ciscoasa(config-ca-server)# lifetime crl 10
```

The local CA updates and reissues the CRL each time that a user certificate is revoked or unrevoked, but if no revocation changes occur, the CRL is reissued automatically once each CRL lifetime. If you do not specify a CRL lifetime, the default time period is six hours.

**Step 3** Force the issuance of a CRL at any time, which immediately updates and regenerates a current CRL to overwrite the existing CRL.

```
crypto ca server crl issue
```

Example:
```
ciscoasa(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
```

**Note** Do not use this command unless the CRL file has been removed in error or has been corrupted and must be regenerated.
Configure the Server Keysize

To configure the server keysize, perform the following steps:

Procedure

**Step 1** Enter local ca server configuration mode.

`crypto ca server`

Example:

```
ciscoasa(config)# crypto ca server
```

**Step 2** Specify the size of the public and private keys generated at user-certificate enrollment.

`keysize server`

Example:

```
ciscoasa(config-ca-server)# keysize server 2048
```

The keypair size options are 512, 768, 1024, 2048 bits, and the default value is 1024 bits.

**Note** After you have enabled the local CA, you cannot change the local CA keysize, because all issued certificates would be invalidated. To change the local CA keysize, you must delete the current local CA and reconfigure a new one.

**Examples**

The following is sample output that shows two user certificates in the database.

Username: user1
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:45:52 UTC Fri Jan 4 2017
Certificates Issued:
serial: 0x71
issued: 12:45:52 UTC Thu Jan 3 2008
expired: 12:17:37 UTC Sun Dec 31 2017
status: Not Revoked
Username: user2
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:27:59 UTC Fri Jan 4 2008
Certificates Issued:
serial: 0x2
issued: 12:27:59 UTC Thu Jan 3 2008
expired: 12:17:37 UTC Sun Dec 31 2017
status: Not Revoked
<--- More --->
Set Up External Local CA File Storage

To configure external local CA file storage, perform the following steps:

**Procedure**

**Step 1**
Access configuration mode for the specific file system type.

```
mount name type
```

Example:
```
ciscoasa(config)# mount mydata type cifs
```

**Step 2**
Mount a CIFS file system.

```
mount name type cifs
```

Example:
```
ciscoasa(config-mount-cifs)# mount mydata type cifs
server 10.1.1.10 share myshare
domain example.com
username user6
password ********
status enable
```

**Note** Only the user who mounts a file system can unmount it with the `no mount` command.

**Step 3**
Enter local CA server configuration mode.

```
crypto ca server
```

Example:
```
ciscoasa(config)# crypto ca server
```

**Step 4**
Specify the location of `mydata`, the premounted CIFS file system to be used for the local CA server database.

```
database path mount-name directory-path
```

Example:
```
ciscoasa(config-ca-server)# database path mydata:newuser
```

This command establishes a path to the server and then specifies the local CA file or folder name to use for storage and retrieval. To return local CA file storage to the ASA flash memory, use the `no database path` command.

**Note** To secure stored local CA files on an external server requires a premounted file system of file type CIFS or FTP that is username-protected and password-protected.

**Step 5**
Save the running configuration.

```
write memory
```

Example:
ciscoasa(config)# write memory

For external local CA file storage, each time that you save the ASA configuration, user information is saved from the ASA to the premounted file system and file location, mydata:newuser.

For flash memory storage, user information is saved automatically to the default location for the start-up configuration.

Examples
The following example shows the list of local CA files that appear in flash memory or in external storage:

ciscoasa(config-ca-server)# dir LOCAL* //
Directory of disk0:/LOCAL*

75 -rwx 32 13:07:49 Jan 20 2007 LOCAL-CA-SERVER.ser
77 -rwx 229 13:07:49 Jan 20 2007 LOCAL-CA-SERVER.cdb
69 -rwx 0 01:09:28 Jan 20 2007 LOCAL-CA-SERVER.udb
81 -rwx 232 19:09:10 Jan 20 2007 LOCAL-CA-SERVER.crl
72 -rwx 1603 01:09:28 Jan 20 2007 LOCAL-CA-SERVER.p12

127119360 bytes total (79693824 bytes free)

Download and Store CRLs

To download and store CRLs, perform the following steps:

Procedure

Step 1 Enter local ca server configuration mode.
crypto ca server

Example:
ciscoasa(config)# crypto ca server

Step 2 Open a port on an interface to make the CRL accessible from that interface. The specified interface and port are used to listen for incoming requests for the CRL.
publish-crl interface interface port portnumber

Example:
ciscoasa(config-ca-server)# publish-crl outside 70

The interface and optional port selections are as follows:

- inside—Name of interface/GigabitEthernet0/1
- management—Name of interface/ Management0/0
- outside—Name of interface/GigabitEthernet0/0
- Port numbers can range from 1-65535. TCP port 80 is the HTTP default port number.
If you do not specify this command, the CRL is not accessible from the CDP location, because this command is required to open an interface to download the CRL file.

The CDP URL can be configured to use the IP address of an interface, and the path of the CDP URL and the filename can also be configured (for example, http://10.10.10.100/user8/my_crl_file).

In this case, only the interface with that IP address configured listens for CRL requests, and when a request comes in, the ASA matches the path, /user8/my_crl_file to the configured CDP URL. When the path matches, the ASA returns the stored CRL file.

The protocol must be HTTP, so the prefix displayed is http://.

Specify the CDP to be included in all issued certificates. If you do not configure a specific location for the CDP, the default URL location is http://hostname.domain/+CSCOCA+/asa_ca.crl.

cdp-url url

Example:

ciscoasa(config-ca-server)# cdp-url http://172.16.1.1/pathname/myca.crl

The local CA updates and reissues the CRL each time a user certificate is revoked or unrevoked. If no revocation changes occur, the CRL is reissued once each CRL lifetime.

If this command is set to serve the CRL directly from the local CA ASA, see Download and Store CRLs, page 34-34 for instructions about opening a port on an interface to make the CRL accessible from that interface.

The CRL exists for other devices to validate the revocation of certificates issued by the local CA. In addition, the local CA tracks all issued certificates and status within its own certificate database. Revocation checking is performed when a validating party needs to validate a user certificate by retrieving the revocation status from an external server, which might be the CA that issued the certificate or a server designated by the CA.

Set Up Enrollment Parameters

To set up enrollment parameters, perform the following steps:

Procedure

Step 1 Enter local ca server configuration mode.
crypto ca server

Example:
ciscoasa(config)# crypto ca server

Step 2 Specify the number of hours that an issued OTP for the local CA enrollment page is valid. The default expiration time is 72 hours.

otp expiration timeout
Example:
ciscoasa(config-ca-server)# otp expiration 24

**Note**  The user OTP to enroll for a certificate on the enrollment website is also used as the password to unlock the PKCS12 file that includes the issued certificate and keypair for the specified user.

**Step 3**  Specify the number of hours an already-enrolled user can retrieve a PKCS12 enrollment file.

**enrollment-retrieval timeout**

Example:
ciscoasa(config-ca-server)# enrollment-retrieval 120

This time period begins when the user is successfully enrolled. The default retrieval period is 24 hours. Valid values for the retrieval period range from 1 to 720 hours. The enrollment retrieval period is independent of the OTP expiration period.

After the enrollment retrieval time expires, the user certificate and keypair are no longer available. The only way a user may receive a certificate is for the administrator to reinitialize certificate enrollment and allow a user to log in again.

### Add and Enroll Users

To add a user who is eligible for enrollment in the local CA database, perform the following steps:

**Procedure**

**Step 1**  Add a new user to the local CA database.

```
crypto ca server user-db add username [dn dn] [email emailaddress]
```

Example:
ciscoasa(config-ca-server)# crypto ca server user-db add user1 dn user1@example.com, Engineer, Example Company, US, email user1@example.com

The **username** argument is a string of 4-64 characters, which is the simple username for the user being added. The username can be an e-mail address, which then is used to contact the user as necessary for enrollment invitations.

The **dn** argument is the distinguished name, a global, authoritative name of an entry in the OSI Directory (X.500) (for example, cn=user1@example.com, cn=Engineer, o=Example Company, c=US).

The **email-address** argument is the e-mail address of the new user to which OTPs and notices are to be sent.

**Step 2**  Provide user privileges to a newly added user.

```
crypto ca server user-db allow user
```

Example:
ciscoasa(config-ca-server)# crypto ca server user-db allow user
Step 3
Notify a user in the local CA database to enroll and download a user certificate, which automatically e-mails the OTP to that user.

```
crypto ca server user-db email-otp username
```

Example:
```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp exampleuser1
```

Note
When an administrator wants to notify a user through e-mail, the administrator must specify the e-mail address in the username field or in the e-mail field when adding that user.

Step 4
Show the issued OTP.

```
crypto ca server user-db show-otp
```

Example:
```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp
```

Step 5
Set the enrollment time limit in hours. The default expiration time is 72 hours.

```
otp expiration timeout
```

Example:
```
ciscoasa(config-ca-server)# otp expiration 24
```

This command defines the amount of time that the OTP is valid for user enrollment. This time period begins when the user is allowed to enroll.

After a user enrolls successfully within the time limit and with the correct OTP, the local CA server creates a PKCS12 file, which includes a keypair for the user and a user certificate that is based on the public key from the keypair generated and the subject-name DN specified when the user is added. The PKCS12 file contents are protected by a passphrase, the OTP. The OTP can be handled manually, or the local CA can e-mail this file to the user to download after the administrator allows enrollment.

The PKCS12 file is saved to temporary storage with the name, `username.p12`. With the PKCS12 file in storage, the user can return within the enrollment-retrieval time period to download the PKCS12 file as many times as needed. When the time period expires, the PKCS12 file is removed from storage automatically and is no longer available to download.

Note
If the enrollment period expires before the user retrieves the PKCS12 file that includes the user certificate, enrollment is not permitted.

Renew Users

To specify the timing of renewal notices, perform the following steps:

Procedure

Step 1
Enter local ca server configuration mode.

```
crypto ca server
```
Guidelines for Digital Certificates

Example:
ciscoasa(config)# crypto ca server

Step 2  Specifies the number of days (1-90) before the local CA certificate expires that an initial reminder to re-enroll is sent to certificate owners.

renewal-reminder time

Example:
ciscoasa(config-ca-server)# renewal-reminder 7

If a certificate expires, it becomes invalid. Renewal notices and the times they are e-mailed to users are variable, and can be configured by the administrator during local CA server configuration.

Three reminders are sent. An e-mail is automatically sent to the certificate owner for each of the three reminders, provided an e-mail address is specified in the user database. If no e-mail address exists for the user, a syslog message alerts you of the renewal requirement.

The ASA automatically grants certificate renewal privileges to any user who holds a valid certificate that is about to expire, as long as the user still exists in the user database. Therefore, if an administrator does not want to allow a user to renew automatically, the administrator must remove the user from the database before the renewal time period.

---

Restore Users

To restore a user and a previously revoked certificate that was issued by the local CA server, perform the following steps:

Procedure

Step 1  Enter local ca server configuration mode.

crypto ca server

Example:
ciscoasa(config)# crypto ca server

Step 2  Restore a user and unrevoke a previously revoked certificate that was issued by the local CA server.

crypto ca server unrevoke cert-serial-no

Example:
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f

The local CA maintains a current CRL with serial numbers of all revoked user certificates. This list is available to external devices and can be retrieved directly from the local CA if it is configured to do so with the cdp-url command and the publish-crl command. When you revoke (or unrevoke) any current certificate by certificate serial number, the CRL automatically reflects these changes.
Remove Users

To delete a user from the user database by username, perform the following steps:

Procedure

Step 1  Enter local ca server configuration mode.
crypto ca server

Example:
ciscoasa(config)# crypto ca server

Step 2  Remove a user from the user database and allow revocation of any valid certificates that were issued to
that user.
crypto ca server user-db remove username

Example:
ciscoasa(config-ca-server)# crypto ca server user-db remove user1

Revoke Certificates

To revoke a user certificate, perform the following steps:

Procedure

Step 1  Enter local ca server configuration mode.
crypto ca server

Example:
ciscoasa(config)# crypto ca server

Step 2  Enter the certificate serial number in hexadecimal format.
crypto ca server revoke cert-serial-no

Example:
ciscoasa(config-ca-server)# crypto ca server revoke 782ea09f

This command marks the certificate as revoked in the certificate database on the local CA server and in
the CRL, which is automatically reissued.

Note The password is also required if the certificate for the ASA needs to be revoked, so make sure
that you record it and store it in a safe place.
Monitoring Digital Certificates

See the following commands for monitoring digital certificate status:

- **show crypto ca server**
  This command shows local CA configuration and status.

- **show crypto ca server cert-db**
  This command shows user certificates issued by the local CA.

- **show crypto ca server certificate**
  This command shows local CA certificates on the console in base 64 format and the rollover certificate when available, including the rollover certificate thumb print for verification of the new certificate during import onto other devices.

- **show crypto ca server crl**
  This command shows CRLs.

- **show crypto ca server user-db**
  This command shows users and their status, which can be used with the following qualifiers to reduce the number of displayed records:
    - **allowed.** Shows only users currently allowed to enroll.
    - **enrolled.** Shows only users that are enrolled and hold a valid certificate
    - **expired.** Shows only users holding expired certificates.
    - **on-hold.** Lists only users without a certificate and not currently allowed to enroll.

- **show crypto ca server user-db allowed**
  This command shows users who are eligible to enroll.

- **show crypto ca server user-db enrolled**
  This command shows enrolled users with valid certificates.

- **show crypto ca server user-db expired**
This command shows users with expired certificates.

- **show crypto ca server user-db on-hold**
  This command shows users without certificates who are not allowed to enroll.

- **show crypto key name of key**
  This command shows key pairs that you have generated.

- **show running-config**
  This command shows local CA certificate map rules.

### Examples

The following example shows an RSA general-purpose key:

```bash
Cisco ASA(config)# show crypto key mypubkey
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:
30819f30 0d06092a 864886f7 0d010101 05000381 80003081 89028181 000ea51b7
0781840f 78bcccac2 41b5b8d 2f3e30b4 4cae9f86 f4485207 159108c9 f5e49103
9eeb0f5d 45fd1811 3baaf0e0ce 292b3b64 b4124a6f 7a77fbb08 75b88df1 8092a9f8
550e9e65 2c271245 7f0d10c3 3aaf1e04 c7c4efa4 600f4c4a 6afe55ad 51d2c01c
e08407dd 459d63e8 8cc0b7ef 14f9e6ac eca141e4 276d7358 f7f50dd13 79020301 0001
```

The following example shows the local CA CRL:

```bash
Cisco ASA(config)# show crypto ca server crl
Certificate Revocation List:
Issuer: cn=xx5520-1-3-2007-1
This Update: 13:32:53 UTC Jan 4 2010
Next Update: 13:32:53 UTC Feb 3 2010
Number of CRL entries: 2
CRL size: 270 bytes
Revoked Certificates:
Serial Number: 0x6f
Revocation Date: 12:30:01 UTC Jan 4 2010
Serial Number: 0x47
Revocation Date: 13:32:48 UTC Jan 4 2010
```

The following example shows one user on-hold:

```bash
Cisco ASA(config)# show crypto ca server user-db on-hold
username: wilma101
e-mail: <None>
dn: <None>
allowed: <not allowed>
notified: 0
```

The following example shows output of the **show running-config** command, in which local CA certificate map rules appear:

```bash
crypto ca certificate map 1
issuer-name co asc
subject-name attr ou eq Engineering
```
## History for Certificate Management

### Table 34-1  History for Certificate Management

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate management</td>
<td>7.0(1)</td>
<td>Digital certificates (including CA certificates, identity certificates, and code signer certificates) provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. CAs are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security.</td>
</tr>
<tr>
<td>Certificate management</td>
<td>7.2(1)</td>
<td>We introduced the following commands: <code>issuer-name DN-string</code>, <code>revocation-check crl none</code>, <code>revocation-check crl</code>, <code>revocation-check none</code>. We deprecated the following commands: `crl { required</td>
</tr>
</tbody>
</table>
Table 34-1 History for Certificate Management (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
</table>
| Certificate management| 8.0(2)            | We introduced the following commands:
|                       |                   | cdp-url, crypto ca server, crypto ca server crl issue, crypto ca server revoke cert-serial-no, crypto ca server unrevoke cert-serial-no, crypto ca server user-db add user [dn dn] [email e-mail-address], crypto ca server user-db allow {username | all-unenrolled | all-certholders} [display-otp] [email-otp] [replace-otp], crypto ca server user-db email-otp {username | all-unenrolled | all-certholders}, crypto ca server user-db remove username, crypto ca server user-db show-otp {username | all-certholders | all-unenrolled}, crypto ca server user-db write, [no] database path mount-name directory-path, debug crypto ca server [level], lifetime {ca-certificate | certificate | crl} time, no shutdown, otp expiration timeout, renewal-reminder time, show crypto ca server, show crypto ca server cert-db [user username | allowed | enrolled | expired | on-hold] [serial certificate-serial-number], show crypto ca server certificate, show crypto ca server crl, show crypto ca server user-db [expired | allowed | on-hold | enrolled], show crypto key name of key, show running-config, shutdown. |
| SCEP proxy            | 8.4(1)            | We introduced this feature, which provides secure deployment of device certificates from third-party CAs. We introduced the following commands:
PART 8

System Administration
Management Access

This chapter describes how to access the Cisco ASA for system management through Telnet, SSH, and HTTPS (using ASDM), how to authenticate and authorize users, and how to create login banners.

- Guidelines for Management Access, page 35-1
- Configure ASA Access for ASDM, Telnet, or SSH, page 35-3
- Configure AAA for System Administrators, page 35-9
- History for Management Access, page 35-27

Guidelines for Management Access

This section describes guidelines and limitations that you should check before configuring management access.

Model Guidelines

For the ASASM, a session from the switch to the ASASM is a Telnet session, but Telnet access configuration according to this section is not required.

VPN Guidelines

For the configurations that follow, 192.168.10.0/24 is the VPN pool for AnyConnect or IPsec VPN clients. Each configuration allows VPN client users to connect to ASDM or SSH to the ASA using the management interface IP address.

- To allow only VPN client users access to ASDM or HTTP (and deny access to all other users), enter the following commands:
  ciscoasa(config)# http server enable
  ciscoasa(config)# http 192.168.10.0 255.255.255.0 management_interface

- To allow only VPN client users access to the ASA using SSH (and deny access to all other users), enter the following command:
  ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface

- You can define only one management access interface.
Additional Guidelines

- To access the ASA interface for management access, you do not also need an access rule allowing the host IP address. You only need to configure management access according to the sections in this chapter.
- You cannot use Telnet to the lowest security interface unless you use Telnet inside a VPN tunnel.
- Management access to an interface other than the one from which you entered the ASA is not supported. For example, if your management host is located on the outside interface, you can only initiate a management connection directly to the outside interface. The only exception to this rule is through a VPN connection.
- The ASA allows:
  - A maximum of 5 concurrent Telnet connections per context, if available, with a maximum of 100 connections divided among all contexts.
  - A maximum of 5 concurrent SSH connections per context, if available, with a maximum of 100 connections divided among all contexts.
  - A maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 32 ASDM instances among all contexts.
- The ASA supports the SSH remote shell functionality provided in SSH Versions 1 and 2 and supports DES and 3DES ciphers.
- XML management over SSL and SSH is not supported.
- (8.4 and later) The SSH default username is no longer supported. You can no longer connect to the ASA using SSH with the pix or asa username and the login password. To use SSH, you must configure AAA authentication using the `aaa authentication ssh console LOCAL` command; then define a local user by entering the `username` command. 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.
- (9.1(2) and later) The default Telnet login password was removed; you must manually set the password before using Telnet.
- To gain access to the ASA CLI using Telnet, enter the login password set by the `password` command. You must manually set the password before using Telnet.
- If you configure Telnet authentication, then enter the username and password defined by the AAA server or local database.
- When starting an SSH session, a dot (.) displays on the ASA console before the following SSH user authentication prompt appears:
  ```
ciscoasa(config)#.
```
  The display of the dot does not affect the functionality of SSH. The dot appears at the console when generating a server key or decrypting a message using private keys during SSH key exchange before user authentication occurs. These tasks can take up to two minutes or longer. The dot is a progress indicator that verifies that the ASA is busy and has not hung. You can alternatively configure a public key instead of using a password.
- If you cannot make a Telnet or SSH connection to the ASA interface, make sure that you enabled Telnet or SSH to the ASA according to the instructions in this chapter.
- From a security perspective, it is important that your banner discourage unauthorized access. Do not use the words “welcome” or “please,” as they appear to invite intruders in. The following banner sets the correct tone for unauthorized access:
Configure ASA Access for ASDM, Telnet, or SSH

This section describes how to configure ASA access for ASDM, Telnet, or SSH.

Configure Telnet Access

To identify the client IP addresses allowed to connect to the ASA using Telnet, perform the following steps:

**Procedure**

**Step 1** Identify the IP addresses from which the ASA accepts connections for each address or subnet.

```
telnet source_IP_address mask source_interface
```

Example:

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

If there is only one interface, you can configure Telnet to access that interface as long as the interface has a security level of 100.

**Step 2** Set the duration for how long a Telnet session can be idle before the ASA disconnects the session.

```
telnet timeout minutes
```

Example:

```
ciscoasa(config)# telnet timeout 30
```

Set the timeout from 1 to 1440 minutes. The default is 5 minutes. The default duration is too short in most cases and should be increased until all pre-production testing and troubleshooting have been completed.
Examples

The following example shows how to let a host on the inside interface with an address of 192.168.1.2 access the ASA:

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

The following example shows how to allow all users on the 192.168.3.0 network to access the ASA on the inside interface:

```
ciscoasa(config)# telnet 192.168.3.0 255.255.255.0 inside
```

Configure SSH Access

To identify the client IP addresses and define a user allowed to connect to the ASA using SSH, perform the following steps:

**Procedure**

**Step 1** Generate an RSA key pair, which is required for SSH (for physical ASAs only).

```
crypto key generate rsa modulus modulus_size
```

Example:

```
ciscoasa(config)# crypto key generate rsa modulus 1024
```

For the ASAv, the RSA key pairs are automatically created after deployment.

The modulus value (in bits) is 512, 768, 1024, or 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA key pair. We recommend a value of 1024.

**Step 2** Save the RSA keys to persistent flash memory.

```
write memory
```

Example:

```
ciscoasa(config)# write memory
```

**Step 3** Enable local authentication for SSH access. You can alternatively configure authentication using a AAA server.

```
aaa authentication ssh console LOCAL
```

Example:

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

**Step 4** Create a user in the local database that can be used for SSH access.

```
username username password password
```

Example:

```
ciscoasa(config)# username user1 password cisco123
```

**Step 5** Identify the IP addresses from which the ASA accepts connections for each address or subnet, and the interface on which you can use SSH. Unlike Telnet, you can SSH on the lowest security level interface.

```
ssh source_IP_address mask source_interface
```
Configure ASA Access for ASDM, Telnet, or SSH

**Example:**
```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

**Step 6**  
(Optional) Set the duration for how long an SSH session can be idle before the ASA disconnects the session.
```
ssh timeout minutes
```

**Example:**
```
ciscoasa(config)# ssh timeout 30
```

Set the timeout from 1 to 60 minutes. The default is 5 minutes. The default duration is too short in most cases, and should be increased until all pre-production testing and troubleshooting have been completed.

**Step 7**  
(Optional) Limit access to SSH version 1 or 2. By default, SSH allows both versions 1 and 2.
```
ssh version version_number
```

**Example:**
```
ciscoasa(config)# ssh version 2
```

**Examples**
The following example shows how to generate RSA keys and let a host on the inside interface with an address of 192.168.1.2 access the ASA:
```
ciscoasa(config)# crypto key generate rsa modulus 1024
write memory
aaa authentication ssh console LOCAL
WARNING: local database is empty! Use 'username' command to define local users.
username exampleuser1 password examplepassword1
ssh 192.168.1.2 255.255.255.255 inside
ssh timeout 30
```

The following example shows how to allow all users on the 192.168.3.0/24 network to access the ASA on the inside interface:
```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

---

Configure HTTPS Access for ASDM

To use ASDM, you need to enable the HTTPS server, and allow HTTPS connections to the ASA. HTTPS access is enabled as part of the factory default configuration or when you use the `setup` command.

To configure HTTPS access for ASDM, perform the following steps:

**Procedure**

**Step 1**  
Identify the IP addresses from which the ASA accepts HTTPS connections for each address or subnet.
```
http source_IP_address mask source_interface
```

**Example:**
```
ciscoasa(config)# http 192.168.1.2
```
Configure ASA Access for ASDM, Telnet, or SSH

Chapter 35 Management Access

Configure ASA Access for ASDM, Telnet, or SSH

Step 2 Enable the HTTPS server.

```
http server enable [port]
```

Example:
```
ciscoasa(config)# http server enable 443
```

By default, the `port` is 443. If you change the port number, be sure to include it in the ASDM access URL. For example, if you change the port number to 444, enter the following:
```
https://10.1.1.1:444
```

Step 3 (Optional) Redirect HTTP requests to HTTPS requests, which makes it possible for users to enter “http://” in the ASDM URL and get to the HTTPS URL without error.

```
http redirect interface [port]
```

Example:
```
ciscoasa(config)# http redirect inside
```

Examples

The following example shows how to enable the HTTPS server and let a host on the inside interface with an address of 192.168.1.2 access ASDM:
```
ciscoasa(config)# http server enable
  ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

The following example shows how to allow all users on the 192.168.3.0/24 network to access ASDM on the inside interface:
```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

Configure a Login Banner

You can configure a message to display when a user connects to the ASA, before a user logs in, or before a user enters privileged EXEC mode.

To configure a login banner, perform the following steps:

Procedure

Step 1 Add a banner to display at one of three times: when a user first connects (message-of-the-day (`motd`)), when a user logs in (`login`), and when a user accesses privileged EXEC mode (`exec`).

```
banner (exec | login | motd) text
```

Example:
```
ciscoasa(config)# banner motd Welcome to $(hostname).
```

When a user connects to the ASA, the message-of-the-day banner appears first, followed by the login banner and prompts. After the user successfully logs in to the ASA, the exec banner appears.

To add more than one line, precede each line by the `banner` command.
For the banner text:

- Spaces are allowed, but tabs cannot be entered using the CLI.
- There are no limits for banner length other than those for RAM and flash memory.
- You can dynamically add the hostname or domain name of the ASA by including the strings $(hostname)$ and $(domain)$.
- If you configure a banner in the system configuration, you can use that banner text within a context by using the $(system)$ string in the context configuration.

Examples

The following example shows how to add a message-of-the-day banner:

```
ciscoasa(config)# banner motd Welcome to $(hostname).
ciscoasa(config)# banner motd Contact me at admin@example.com for any
issues.
```

Customize a CLI Prompt

The CLI Prompt pane lets you customize the prompt used during CLI sessions. By default, the prompt shows the hostname of the ASA. In multiple context mode, the prompt also displays the context name. You can display the following items in the CLI prompt:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-unit</td>
<td>(Single and multiple mode) Displays the cluster unit name. Each unit in a</td>
</tr>
<tr>
<td></td>
<td>cluster can have a unique name.</td>
</tr>
<tr>
<td>context</td>
<td>(Multiple mode only) Displays the name of the current context.</td>
</tr>
<tr>
<td>domain</td>
<td>Displays the domain name.</td>
</tr>
<tr>
<td>hostname</td>
<td>Displays the hostname.</td>
</tr>
<tr>
<td>priority</td>
<td>Displays the failover priority as pri (primary) or sec (secondary).</td>
</tr>
<tr>
<td>state</td>
<td>Displays the traffic-passing state of the unit. The following values appear for the state:</td>
</tr>
<tr>
<td></td>
<td>• act—Failover is enabled, and the unit is actively passing traffic.</td>
</tr>
<tr>
<td></td>
<td>• stby—Failover is enabled, and the unit is not passing traffic and is in a</td>
</tr>
<tr>
<td></td>
<td>standby, failed, or another inactive state.</td>
</tr>
<tr>
<td></td>
<td>• actNoFailover—Failover is not enabled, and the unit is actively passing</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td></td>
<td>• stbyNoFailover—Failover is not enabled, and the unit is not passing</td>
</tr>
<tr>
<td></td>
<td>traffic. This condition might occur when there is an interface failure</td>
</tr>
<tr>
<td></td>
<td>above the threshold on the standby unit.</td>
</tr>
<tr>
<td></td>
<td>Shows the role (master or slave) of a unit in a cluster. For example, in the</td>
</tr>
<tr>
<td></td>
<td>prompt ciscoasa/cl2/slave, the hostname is ciscoasa, the unit name is cl2,</td>
</tr>
<tr>
<td></td>
<td>and the state name is slave.</td>
</tr>
</tbody>
</table>

To customize the CLI prompt, perform the following steps:
Configure ASA Access for ASDM, Telnet, or SSH

Chapter 35  Management Access

Configure ASA Access for ASDM, Telnet, or SSH

Procedure

Step 1
Customize the CLI prompt by entering the following command:

```
prompt { [hostname] [context] [domain] [slot] [state] [priority] [cluster-unit] }
```

Example:

```
ciscoasa(config)# firewall transparent
```

Change the Console Timeout

The console timeout sets how long a connection can remain in privileged EXEC mode or configuration mode; when the timeout is reached, the session drops into user EXEC mode. By default, the session does not time out. This setting does not affect how long you can remain connected to the console port, which never times out.

To change the console timeout, perform the following steps:

Procedure

Step 1
Specify the idle time in minutes (0 through 60) after which the privileged session ends. The default timeout is 0, which means the session does not time out.

```
console timeout number
```

Example:

```
ciscoasa(config)# console timeout 0
```

Configure Management Access Over a VPN Tunnel

If your VPN tunnel terminates on one interface, but you want to manage the ASA by accessing a different interface, you can identify that interface as a management-access interface. For example, if you enter the ASA from the outside interface, this feature lets you connect to the inside interface using ASDM, SSH, Telnet, or SNMP; or you can ping the inside interface when entering from the outside interface.

Management access is available via the following VPN tunnel types: IPsec clients, IPsec site-to-site, and the AnyConnect SSL VPN client.

To configure a management interface, perform the following steps:

Procedure

Step 1
Specify the name of the management interface that you want to access when entering the ASA from another interface.

```
management-access management_interface
```

Example:

```
ciscoasa(config)# management-access inside
```
Configure AAA for System Administrators

This section describes how to enable authentication and command authorization for system administrators.

CLI Access with and without Authentication

How you log into the ASA depends on whether or not you enable authentication:

- **No Authentication**—If you do not enable any authentication for Telnet, you do not enter a username; you enter the login password (set with the `password` command). (SSH is not available without authentication). You access user EXEC mode.

- **Authentication**—If you enable Telnet or SSH authentication according to this section, you enter the username and password as defined on the AAA server or local user database. You access user EXEC mode.

To enter privileged EXEC mode after logging in, enter the `enable` command. How `enable` works depends on whether you enable authentication:

- **No Authentication**—If you do not configure enable authentication, enter the system enable password when you enter the `enable` command (set by the `enable password` command). However, if you do not use enable authentication, after you enter the `enable` command, you are no longer logged in as a particular user. To maintain your username, use enable authentication.

- **Authentication**—If you configure enable authentication (see Configure Authentication to Access Privileged EXEC Mode, page 35-13), the ASA prompts you for your username and password again. This feature is particularly useful when you perform command authorization, in which usernames are important in determining the commands that a user can enter.

For enable authentication using the local database, you can use the `login` command instead of the `enable` command. `login` maintains the username but requires no configuration to turn on authentication.

ASDM Access with and without Authentication

By default, you can log into ASDM with a blank username and the enable password set by the `enable password` command. Note that if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

If you configure HTTP authentication, you can no longer use ASDM with a blank username and the enable password.
Sessions from the Switch to the ASA Services Module

For sessions from the switch to the ASASM (using the session command), you can configure Telnet authentication. For virtual console connections from the switch to the ASASM (using the service-module session command), you can configure serial port authentication.

In multiple context mode, you cannot configure any AAA commands in the system configuration. However, if you configure Telnet or serial authentication in the admin context, then authentication also applies to sessions from the switch to the ASASM. The admin context AAA server or local user database is used in this instance.

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the ASA. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the ASA places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the assigned privilege level and below. Note that all users access user EXEC mode when they first log in (commands at level 0 or 1). The user needs to authenticate again with the enable command to access privileged EXEC mode (commands at level 2 or higher), or they can log in with the login command (local database only).

  Note  You can use local command authorization without any users in the local database and without CLI or enable authentication. Instead, when you enter the enable command, you enter the system enable password, and the ASA places you in level 15. You can then create enable passwords for every level, so that when you enter enable n (2 to 15), the ASA places you in level n. These levels are not used unless you enable local command authorization.

- TACACS+ server privilege levels—On the TACACS+ server, configure the commands that a user or group can use after authenticating for CLI access. Every command that a user enters at the CLI is validated with the TACACS+ server.

Preserve User Credentials

When a user logs into the ASA, that user is required to provide a username and password for authentication. The ASA retains these session credentials in case further authentication is needed later in the session.

When the following configurations are in place, a user needs only to authenticate with the local server for login. Subsequent serial authorization uses the saved credentials. The user is also prompted for the privilege level 15 password. When exiting privileged mode, the user is authenticated again. User credentials are not retained in privileged mode.

- The local server is configured to authenticate user access.
- Privilege level 15 command access is configured to require a password.
- The user account is configured for serial-only authorization (no access to console or ASDM).
- The user account is configured for privilege level 15 command access.
The following table shows how credentials are used in this case by the ASA.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Password</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Privileged Mode Password</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Security Contexts and Command Authorization**

The following are important points to consider when implementing command authorization with multiple security contexts:

- AAA settings are discrete per context, not shared among contexts.
  - When configuring command authorization, you must configure each security context separately. This configuration provides you the opportunity to enforce different command authorizations for different security contexts.
  - When switching between security contexts, administrators should be aware that the commands permitted for the username specified when they login may be different in the new context session or that command authorization may not be configured at all in the new context. Failure to understand that command authorizations may differ between security contexts could confuse an administrator. This behavior is further complicated by the next point.
  - New context sessions started with the `changeto` command always use the default enable_15 username as the administrator identity, regardless of which username was used in the previous context session. This behavior can lead to confusion if command authorization is not configured for the enable_15 user or if authorizations are different for the enable_15 user than for the user in the previous context session.
  - This behavior also affects command accounting, which is useful only if you can accurately associate each command that is issued with a particular administrator. Because all administrators with permission to use the `changeto` command can use the enable_15 username in other contexts, command accounting records may not readily identify who was logged in as the enable_15 username. If you use different accounting servers for each context, tracking who was using the enable_15 username requires correlating the data from several servers.
  - When configuring command authorization, consider the following:
    - An administrator with permission to use the `changeto` command effectively has permission to use all commands permitted to the enable_15 user in each of the other contexts.
    - If you intend to authorize commands differently per context, ensure that in each context the enable_15 username is denied use of commands that are also denied to administrators who are permitted use of the `changeto` command.
  - When switching between security contexts, administrators can exit privileged EXEC mode and enter the `enable` command again to use the username that they need.

**Note**

The system execution space does not support AAA commands; therefore, command authorization is not available in the system execution space.
Command Privilege Levels

By default, the following commands are assigned to privilege level 0. All other commands are assigned to privilege level 15.

- show checksum
- show curpriv
- enable
- help
- show history
- login
- logout
- pager
- show pager
- clear pager
- quit
- show version

If you move any configure mode commands to a lower level than 15, be sure to move the configure command to that level as well, otherwise, the user cannot enter configuration mode.

Configure Authentication for CLI and ASDM Access

This section describes how to configure authentication for CLI, ASDM, and enable command access.

Before You Begin

- Configure Telnet, SSH, or HTTP access.
- You must configure SSH authentication to obtain SSH access; there is no default username.

To configure authentication for CLI, ASDM, and enable command access, perform the following steps:

Procedure

Step 1
Authenticate users for management access.

```
aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]}
```

Example:

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
ciscoasa(config)# aaa authentication serial console LOCAL
```

The `telnet` keyword controls Telnet access. For the ASASM, this keyword also affects the session from the switch using the `session` command. The `ssh` keyword controls SSH access. The `http` keyword controls ASDM access. The `serial` keyword controls console port access. For the ASASM, this keyword affects the virtual console accessed from the switch using the `service-module session` command.

HTTP management authentication does not support the SDI protocol for a AAA server group.
If you use a AAA server group for authentication, you can configure the ASA to use the local database as a fallback method if the AAA server is unavailable. Specify the server group name followed by LOCAL (LOCAL is case sensitive). We recommend that you use the same username and password in the local database as the AAA server, because the ASA prompt does not give any indication which method is being used. You can alternatively use the local database as your primary method of authentication (with no fallback) by entering LOCAL alone.

**Step 2** Request a certificate from ASDM clients connecting over HTTP on the specified interface.

```
http authentication-certificate interface
```

Example:
```
ciscoasa(config)# http authentication-certificate inside
```

You can use this command in addition to the `aaa authentication` command for ASDM. This command is only for ASDM access, use the `ssl certificate-authentication` command to require a certificate for all other SSL traffic (for example, cut-through proxy).

---

### Configure Authentication to Access Privileged EXEC Mode

Choose one of the following options for authenticating users:

To authenticate users with a AAA server or the local database, perform the following steps:

**Procedure**

**Step 1** Enter the following command:

```
aaa authentication enable console (LOCAL | server_group [LOCAL])
```

Example:
```
ciscoasa(config)# aaa authentication enable console LOCAL
```

The user is prompted for the username and password.

If you use a AAA server group for authentication, you can configure the ASA to use the local database as a fallback method if the AAA server is unavailable. Specify the server group name followed by LOCAL (LOCAL is case sensitive). We recommend that you use the same username and password in the local database as the AAA server, because the ASA prompt does not give any indication of which method is being used. You can alternatively use the local database as your primary method of authentication (with no fallback) by entering LOCAL alone.

To log in as a user from the local database, perform the following steps:

**Step 1** Enter the following command:

```
login
```

Example:
```
ciscoasa# login
```
The ASA prompts for your username and password. After you enter your password, the ASA places you in the privilege level that the local database specifies.

Users can log in with their own username and password to access privileged EXEC mode, so you do not have to provide the system enable password to everyone. To allow users to access privileged EXEC mode (and all commands) when they log in, set the user privilege level to 2 (the default) through 15. If you configure local command authorization, then the user can only enter commands assigned to that privilege level or lower.

**Caution**

If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged EXEC mode, you should configure command authorization. Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use a AAA server for authentication, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged EXEC mode.

---

**Limit User CLI and ASDM Access with Management Authorization**

The ASA enables you to distinguish between administrative and remote-access users when they authenticate using RADIUS, LDAP, TACACS+, or the local user database. User role differentiation can prevent remote access VPN and network access users from establishing an administrative connection to the ASA.

**Note**

Serial access is not included in management authorization, so if you configure the `aaa authentication serial console` command, then any user who authenticates can access the console port.

**Procedure**

**Step 1**

To enable management authorization for local, RADIUS, LDAP (mapped), and TACACS+ users, enter the following command:

```bash
ciscoasa(config)# aaa authorization exec {authentication-server | LOCAL} [auto-enable]
```

When the **LOCAL** option is configured, the local user database is the source for the username entered and the Service-Type and Privilege-Level attributes assigned.

This option also enables support of administrative user privilege levels from RADIUS, which can be used in conjunction with local command privilege levels for command authorization.

When the **authentication-server** option is configured, the same server is used for both authentication and authorization.

The **auto-enable** option allows users with sufficient privileges from the login authentication server to be placed directly in privileged EXEC mode. Otherwise, users are placed in user EXEC mode. These privileges are determined by the Service-Type and Privilege-Level attributes that are required to enter each EXEC mode. To enter privileged EXEC mode, users must have a Service-Type attribute of Administrative and a Privilege Level attribute of greater than 1 assigned to them.
This option is not supported in the system context. However, if you configure Telnet or serial
authentication in the admin context, then authentication also applies to sessions from the switch to
the ASASM.

There is no effect if you enter the `aaa authorization exec` command alone.

The `auto-enable` option is not included when you use serial authentication in management
authorization.

The `aaa authentication http` command is not affected by the `auto-enable` option.

Before you configure the `auto-enable` option, we recommend that you configure both protocol login
and enable authentication, and that all authentication requests go to the same AAA server group, as
shown in the following example:

```
ciscoasa (config)# aaa authentication ssh console RADIUS
```

```
ciscoasa (config)# aaa authentication enable console RADIUS
```

```
ciscoasa (config)# aaa authorization exec authentication-server auto-enable
```

We do not recommend that you use other types of configurations.

**Step 2**

To configure the user for management authorization, see the following requirements for each AAA
server type or local user:

- **RADIUS or LDAP (mapped) users**

  When users are authenticated through LDAP, the native LDAP attributes and their values can be
  mapped to Cisco ASA attributes to provide specific authorization features. Configure Cisco VSA
  CVPN3000-Privilege-Level with a value between 0 and 15, and then map the LDAP attributes to
  Cisco VAS CVPN3000-Privilege-Level using the `ldap map-attributes` command.

  The RADIUS IETF `service-type` attribute, when sent in an access-accept message as the result of a
  RADIUS authentication and authorization request, is used to designate which type of service is
  granted to the authenticated user:

  - **Service-Type 6 (Administrative)**—Allows full access to any services specified by the `aaa
    authentication console` commands.

  - **Service-Type 7 (NAS prompt)**—Allows access to the CLI when you configure the `aaa
    authentication {telnet | ssh} console` command, but denies ASDM configuration access if you
    configure the `aaa authentication http console` command. ASDM monitoring access is allowed.
    If you configure `enable` authentication with the `aaa authentication enable console` command,
    the user cannot access privileged EXEC mode using the `enable` command. The Framed (2) and
    Login (1) service types are treated the same way.

  - **Service-Type 5 (Outbound)**—Denies management access. The user cannot use any services
    specified by the `aaa authentication console` commands(excluding the `serial` keyword; serial
    access is allowed). Remote access (IPsec and SSL) users can still authenticate and terminate
    their remote access sessions. All other service types (Voice, FAX, and so on) are treated the
    same way.

  The RADIUS Cisco VSA `privilege-level` attribute (Vendor ID 3076, sub-ID 220), when sent in an
  access-accept message, is used to designate the level of privilege for the user.

  When an authenticated user tries administrative access to the ASA through ASDM, SSH, or Telnet,
  but does not have the appropriate privilege level to do so, the ASA generates syslog message
  113021. This message informs the user that the attempted login failed because of inappropriate
  administrative privileges.

  The following example shows how to define an LDAP attribute map. In this example, the security
  policy specifies that users being authenticated through LDAP map the user record fields or
  parameters title and company to the IETF-RADIUS service-type and privilege-level, respectively.
The following example applies an LDAP attribute map to an LDAP AAA server:

ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1

ciscoasa(config-aaa-server-host)# ldap-attribute-map admin-control

- **TACACS+ users**
  
  Authorization is requested with “service=shell,” and the server responds with PASS or FAIL.

  - PASS, privilege level 1—Allows access to ASDM, with limited read-only access to the configuration and monitoring sections, and access for show commands that are privilege level 1 only.
  
  - PASS, privilege level 2 and higher—Allows access to the CLI when you configure the aaa authentication {telnet | ssh} console command, but denies ASDM configuration access if you configure the aaa authentication http console command. ASDM monitoring access is allowed. If you configure enable authentication with the aaa authentication enable console command, the user cannot access privileged EXEC mode using the enable command. You are not allowed to access privileged EXEC mode using the enable command if your enable privilege level is set to 14 or less.
  
  - FAIL—Denies management access. You cannot use any services specified by the aaa authentication console commands(excluding the serial keyword; serial access is allowed).

- **Local users**
  
  Set the service-type command for a given username. By default, the service-type is admin, which allows full access to any services specified by the aaa authentication console command.

---

### Configure a Password Policy for Local Database Users

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.

The password policy only applies to administrative users using the local database, and not to other types of traffic that can use the local database, such as VPN or AAA for network access, and not to users authenticated by a AAA server.

After you configure the password policy, when you change a password (either your own or another user’s), the password policy applies to the new password. Any existing passwords are grandfathered in. The new policy applies to changing the password with the username command as well as the change-password command.

**Before You Begin**

- Configure both CLI/ASDM and enable authentication.
- Specify the local database.

**Procedure**

**Step 1** (Optional) Set the interval in days after which passwords expire for remote users (SSH, Telnet, HTTP).
password-policy lifetime days

Example:
ciscoasa(config)# password-policy lifetime 180

Note Users at the console port are never locked out because of password expiration.

Valid values are between 0 and 65536 days. The default value is 0 days, a value indicating that passwords will never expire.

Seven days before the password expires, a warning message appears. After the password expires, system access is denied to remote users. To gain access after expiration, do one of the following:

- Have another administrator change your password with the username command.
- Log in to the physical console port to change your password.

Step 2 (Optional) Set the minimum number of characters that you must change between new and old passwords.

password-policy minimum-changes value

Example:
ciscoasa(config)# password-policy minimum-changes 2

Valid values are between 0 and 64 characters. The default value is 0.

Character matching is position independent, meaning that new password characters are considered changed only if they do not appear anywhere in the current password.

Step 3 (Optional) Set the minimum length of passwords.

password-policy minimum-length value

Example:
ciscoasa(config)# password-policy minimum-length 8

Valid values are between 3 and 64 characters. We recommend a minimum password length of 8 characters.

Step 4 (Optional) Set the minimum number of upper case characters that passwords must have.

password-policy minimum-uppercase value

Example:
ciscoasa(config)# password-policy minimum-uppercase 3

Valid values are between 0 and 64 characters. The default value is 0, which means there is no minimum.

Step 5 (Optional) Set the minimum number of lower case characters that passwords must have.

password-policy minimum-lowercase value

Example:
ciscoasa(config)# password-policy minimum-lowercase 6

Valid values are between 0 and 64 characters. The default value is 0, which means there is no minimum.

Step 6 (Optional) Set the minimum number of numeric characters that passwords must have.

password-policy minimum-numeric value
Configure AAA for System Administrators

Example:
```
ciscoasa(config)# password-policy minimum-numeric 1
```

Valid values are between 0 and 64 characters. The default value is 0, which means there is no minimum.

**Step 7** (Optional) Set the minimum number of special characters that passwords must have.

```
password-policy minimum-special value
```

Example:
```
ciscoasa(config)# password-policy minimum-special 2
```

Valid values are between 0 and 64 characters. Special characters include the following: !, @, #, $, %, ^, &, *, '(' and ')'. The default value is 0, which means there is no minimum.

**Step 8** (Optional) Set whether users must change their password using the `change-password` command, instead of letting users change their password with the `username` command.

```
password-policy authenticate enable
```

Example:
```
ciscoasa(config)# password-policy authenticate enable
```

The default setting is disabled: a user can use either method to change their password.

If you enable this feature and try to change your password with the `username` command, the following error message appears:

```
ERROR: Changing your own password is prohibited
```

You also cannot delete your own account with the `clear configure username` command. If you try, the following error message appears:

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

### Change Your Password

If you configure a password lifetime in the password policy, you need to change your username password to a new one when the old password expires. This password change method is required if you enable password policy authentication. If password policy authentication is not enabled, then you can use this method, or you can change your user account directly.

To change your username password, perform the following steps:

**Procedure**

**Step 1** Enter the following command:
```
change-password [old-password old_password [new-password new_password]]
```

Example:
```
ciscoasa# change-password old-password johncrichton new-password a3rynsun
```

If you do not enter the old and new passwords in the command, the ASA prompts you for input.
Configure Command Authorization

If you want to control access to commands, the ASA lets you configure command authorization, where you can determine which commands that are available to a user. By default when you log in, you can access user EXEC mode, which offers only minimal commands. When you enter the enable command (or the login command when you use the local database), you can access privileged EXEC mode and advanced commands, including configuration commands.

You can use one of two command authorization methods:

- Local privilege levels
- TACACS+ server privilege levels

Configure Local Command Authorization

Local command authorization lets you assign commands to one of 16 privilege levels (0 to 15). By default, each command is assigned either to privilege level 0 or 15. You can define each user to be at a specific privilege level, and each user can enter any command at the assigned privilege level or below. The ASA supports user privilege levels defined in the local database, a RADIUS server, or an LDAP server (if you map LDAP attributes to RADIUS attributes).

To configure local command authorization, perform the following steps:

Procedure

**Step 1** Assign a command to a privilege level.

```
privilege [show | clear | cmd] level level [mode {enable | cmd}] command command
```

Example:

```
ciscoasa(config)# privilege show level 5 command filter
```

Repeat this command for each command that you want to reassign.

The options in this command are the following:

- **show | clear | cmd**—These optional keywords let you set the privilege only for the show, clear, or configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the show or clear prefix) or as the no form. If you do not use one of these keywords, all forms of the command are affected.

- **level level**—A level between 0 and 15.

- **mode {enable | configure}**—If a command can be entered in user EXEC or privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately:
  - **enable**—Specifies both user EXEC mode and privileged EXEC mode.
  - **configure**—Specifies configuration mode, accessed using the configure terminal command.

**Step 2** Support administrative user privilege levels from RADIUS and enforce user-specific access levels for users who authenticate for management access.

```
aaa authorization exec authentication-server
```
Example:

ciscoasa(config)# aaa authorization exec authentication-server

Without this command, the ASA only supports privilege levels for local database users and defaults all other types of users to level 15.

This command also enables management authorization for local, RADIUS, LDAP (mapped), and TACACS+ users.

Use the **aaa authorization exec LOCAL** command to enable attributes to be taken from the local database.

**Step 3**  
Enable the use of local command privilege levels, which can be checked with the privilege level of users in the local database, RADIUS server, or LDAP server (with mapped attributes).

**aaa authorization command LOCAL**

Example:

ciscoasa(config)# aaa authorization command LOCAL

When you set command privilege levels, command authorization does not occur unless you configure command authorization with this command.

**Examples**

The **filter** command has the following forms:

- **filter** (represented by the **configure** option)
- **show running-config filter**
- **clear configure filter**

You can set the privilege level separately for each form, or set the same privilege level for all forms by omitting this option. The following example shows how to set each form separately:

```
ciscoasa(config)# privilege show level 5 command filter
```
```
ciscoasa(config)# privilege clear level 10 command filter
```
```
ciscoasa(config)# privilege cmd level 10 command filter
```

Alternatively, the following example shows how to set all filter commands to the same level:

```
ciscoasa(config)# privilege level 5 command filter
```

The **show privilege** command separates the forms in the display.

The following example shows the use of the **mode** keyword. The **enable** command must be entered from user EXEC mode, while the **enable password** command, which is accessible in configuration mode, requires the highest privilege level:

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
```
```
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
```
```
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

The following example shows an additional command, the **configure** command, which uses the **mode** keyword:

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
```
```
ciscoasa(config)# privilege clear level 15 mode cmd command configure
```
```
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
```
```
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```
Configure Commands on the TACACS+ Server

You can configure commands on a Cisco Secure Access Control Server (ACS) TACACS+ server as a shared profile component, for a group, or for individual users. For third-party TACACS+ servers, see your server documentation for more information about command authorization support.

See the following guidelines for configuring commands in Cisco Secure ACS Version 3.1; many of these guidelines also apply to third-party servers:

- The ASA sends the commands to be authorized as shell commands, so configure the commands on the TACACS+ server as shell commands.

Note: Cisco Secure ACS might include a command type called “pix-shell.” Do not use this type for ASA command authorization.

- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by permit or deny.

  For example, to allow the `show running-configuration aaa-server` command, add `show running-configuration` to the command field, and type `permit aaa-server` in the arguments field.

- You can permit all arguments of a command that you do not explicitly deny by checking the Permit Unmatched Args check box.

  For example, you can configure just the `show` command, then all the `show` commands are allowed. We recommend using this method so that you do not have to anticipate every variant of a command, including abbreviations and a question mark, which shows CLI usage.

- For commands that are a single word, you must permit unmatched arguments, even if there are no arguments for the command, for example `enable` or `help`.

- To disallow some arguments, enter the arguments preceded by deny.

  For example, to allow `enable`, but not `enable password`, enter `enable` in the commands field, and `deny password` in the arguments field. Be sure to check the Permit Unmatched Args check box so that `enable` alone is still allowed.

- When you abbreviate a command at the command line, the ASA expands the prefix and main command to the full text, but it sends additional arguments to the TACACS+ server as you enter them.

  For example, if you enter `sh log`, then the ASA sends the entire command to the TACACS+ server, `show logging`. However, if you enter `sh log mess`, then the ASA sends `show logging mess` to the TACACS+ server, and not the expanded command `show logging message`. You can configure multiple spellings of the same argument to anticipate abbreviations.

- We recommend that you allow the following basic commands for all users:
  - `show checksum`
  - `show curpriv`
  - `enable`
  - `help`
  - `show history`
Configure AAA for System Administrators

- login
- logout
- pager
- show pager
- clear pager
- quit
- show version

Configure TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the ASA sends the command and username to the TACACS+ server to determine if the command is authorized.

Before you enable TACACS+ command authorization, be sure that you are logged into the ASA as a user that is defined on the TACACS+ server, and that you have the necessary command authorization to continue configuring the ASA. For example, you should log in as an admin user with all commands authorized. Otherwise, you could become unintentionally locked out.

Do not save your configuration until you are sure that it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the ASA. If you still get locked out, see Recover from a Lockout, page 35-25.

Be sure that your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the ASA. For example, in your TACACS+ server pool, include one server connected to interface 1, and another to interface 2. You can also configure local command authorization as a fallback method if the TACACS+ server is unavailable. In this case, you need to configure local users and command privilege levels according to procedures listed in the Configure Command Authorization, page 35-19.

To configure command authorization using a TACACS+ server, perform the following steps:

Procedure

**Step 1**

Enter the following command:

```plaintext
aaa authorization command tacacs+_server_group [LOCAL]
```

Example:

```plaintext
ciscoasa(config)# aaa authorization command group_1 LOCAL
```

You can configure the ASA to use the local database as a fallback method if the TACACS+ server is unavailable. To enable fallback, specify the server group name followed by LOCAL (LOCAL is case sensitive). We recommend that you use the same username and password in the local database as the TACACS+ server because the ASA prompt does not give any indication of which method is being used. Be sure to configure users in the local database and command privilege levels.
Configure Management Access Accounting

You can send accounting messages to the TACACS+ accounting server when you enter any command other than `show` commands at the CLI. You can configure accounting when users log in, when they enter the `enable` command, or when they issue commands.

For command accounting, you can only use TACACS+ servers.

To configure management access and enable command accounting, perform the following steps:

**Procedure**

**Step 1** Enter the following command:

```
aaa accounting {serial | telnet | ssh | enable} console server-tag
```

Example:

```
ciscoasa(config)# aaa accounting telnet console group_1
```

Valid server group protocols are RADIUS and TACACS+.

**Step 2** Enable command accounting. Only TACACS+ servers support command accounting.

```
aaa accounting command [privilege level] server-tag
```

Example:

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

The `privilege level` keyword-argument pair is the minimum privilege level and the `server-tag` argument is the name of the TACACS+ server group to which the ASA should send command accounting messages.

Set a Management Session Quota

You can establish a maximum number of simultaneous ASDM, SSH, and Telnet sessions that are allowed on the ASA. If the maximum is reached, no additional sessions are allowed and a syslog message is generated. To prevent a system lockout, the management session quota mechanism cannot block a console session.

To set a management session quota, perform the following steps:

**Procedure**

**Step 1** Enter the following command:

```
quota management-session number
```

Example:

```
ciscoasa(config)# quota management-session 1000
```

Entering the `no` form of this command sets the quota value to 0, which means that there is no session limit. Valid values range from 0 to 10000.
Exchange Keys in an SSH Session

The Diffie-Hellman (DH) key exchange provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication.

Both the DH Group 1 and Group 14 key-exchange methods for key exchange are supported on the ASA. If no DH group key-exchange method is specified, the DH group 1 key-exchange method is used. For more information about using DH key-exchange methods, see RFC 4253.

To exchange keys in an SSH session, perform the following steps:

---

**Step 1**

Enter the following command:

```
ssh key-exchange group {dh-group1 | dh-group14} sha-1
```

Example:

```
ciscoasa(config)# ssh key-exchange group dh-group14 sha-1
ciscoasa# show running-config key-exchange
ssh key-exchange dh-group14-sha1
```

The `key-exchange` keyword specifies that either the DH group 1 or DH group 14 key-exchange method will follow and should be used when exchanging keys.

The `group` keyword indicates that either the DH group 1 key-exchange method or the DH group 14 key-exchange method will follow and should be used when exchanging keys.

The `dh-group1` keyword indicates that the DH group 1 key-exchange method will follow and should be used when exchanging keys. DH group 2 is called DH group 1 for legacy reasons.

The `dh-group14` keyword indicates that the DH group 14 key-exchange method will follow and should be used when exchanging keys.

The `sha-1` keyword indicates that the SHA-1 encryption algorithm should be used.

Use the `show running-config ssh key-exchange` command to display the DH group key-exchange method currently being used.
Recover from a Lockout

In some circumstances, when you turn on command authorization or CLI authentication, you can be locked out of the ASA CLI. You can usually recover access by restarting the ASA. However, if you already saved your configuration, you might be locked out.

Table 35-1 lists the common lockout conditions and how you might recover from them.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Lockout Condition</th>
<th>Description</th>
<th>Workaround: Single Mode</th>
<th>Workaround: Multiple Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local CLI authentication</td>
<td>No users have been configured in the local database.</td>
<td>If you have no users in the local database, you cannot log in, and you cannot add any users.</td>
<td>Log in and reset the passwords and aaa commands.</td>
<td>Session into the ASA from the switch. From the system execution space, you can change to the context and add a user.</td>
</tr>
<tr>
<td>TACACS+ command authorization</td>
<td>The server is down or unreachable and you do not have the fallback method configured.</td>
<td>If the server is unreachable, then you cannot log in or enter any commands.</td>
<td>1. Log in and reset the passwords and AAA commands. 2. Configure the local database as a fallback method so you do not get locked out when the server is down.</td>
<td>1. If the server is unreachable because the network configuration is incorrect on the ASA, session into the ASA from the switch. From the system execution space, you can change to the context and reconfigure your network settings. 2. Configure the local database as a fallback method so that you do not get locked out when the server is down.</td>
</tr>
<tr>
<td>TACACS+ CLI authentication</td>
<td>You are logged in as a user without enough privileges or as a user that does not exist.</td>
<td>You enable command authorization, but then find that the user cannot enter any more commands.</td>
<td>Fix the TACACS+ server user account.  If you do not have access to the TACACS+ server and you need to configure the ASA immediately, then log into the maintenance partition and reset the passwords and aaa commands.</td>
<td>Session into the ASA from the switch. From the system execution space, you can change to the context and complete the configuration changes. You can also disable command authorization until you fix the TACACS+ configuration.</td>
</tr>
<tr>
<td>RADIUS CLI authentication</td>
<td>You are logged in as a user without enough privileges.</td>
<td>You enable command authorization, but then find that the user cannot enter any more commands.</td>
<td>Log in and reset the passwords and aaa commands.</td>
<td>Session into the ASA from the switch. From the system execution space, you can change to the context and change the user level.</td>
</tr>
</tbody>
</table>

See the following commands for monitoring device access:

- `show running-config all privilege all`
This command shows privilege levels for all commands.

- **show running-config privilege level level**
  
  This command shows commands for a specific privilege level. The *level* argument is an integer between 0 and 15.

- **show running-config privilege command command**
  
  This command shows the privilege level of a specific command.

**Examples**

For the **show running-config all privilege all** command, the ASA displays the current assignment of each CLI command to a privilege level. The following is sample output from this command:

```bash
Ciscoasa(config)# show running-config all privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
... 
```

The following example shows the command assignments for privilege level 10:

```bash
Ciscoasa(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

The following example shows the command assignments for the **access-list** command:

```bash
Ciscoasa(config)# show running-config privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**
  
  This command shows the currently logged-in user.

**Examples**

The following is sample output from the **show curpriv** command:

```bash
Ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```
Table 35-2 describes the show curpriv command output.

### Table 35-2  show curpriv Command Output Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Username. If you are logged in as the default user, the name is enable_1 (user EXEC) or enable_15 (privileged EXEC).</td>
</tr>
<tr>
<td>Current privilege level</td>
<td>Levels range from 0 to 15. Unless you configure local command authorization and assign commands to intermediate privilege levels, levels 0 and 15 are the only levels that are used.</td>
</tr>
<tr>
<td>Current Modes</td>
<td>The available access modes are the following:</td>
</tr>
<tr>
<td></td>
<td>• P_UNPR—User EXEC mode (levels 0 and 1)</td>
</tr>
<tr>
<td></td>
<td>• P_PRIV—Privileged EXEC mode (levels 2 to 15)</td>
</tr>
<tr>
<td></td>
<td>• P_CONF—Configuration mode</td>
</tr>
</tbody>
</table>

### History for Management Access

Table 35-3  History for Management Access

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Access</td>
<td>7.0(1)</td>
<td>We introduced this feature. We introduced the following commands: show running-config all privilege all, show running-config privilege level, show running-config privilege command, telnet, telnet timeout, ssh, ssh timeout, http, http server enable, asdm image disk, banner, console timeout, icmp, ipv6 icmp, management access, aaa authentication console, aaa authentication enable console, aaa authentication telnet</td>
</tr>
</tbody>
</table>
Increased SSH security; the SSH default username is no longer supported.

Starting in 8.4(2), you can no longer connect to the ASA using SSH with the pix or asa username and the login password. To use SSH, you must configure AAA authentication using the `aaa authentication ssh console LOCAL` command (CLI) or Configuration > Device Management > Users/AAA > AAA Access > Authentication (ASDM); then define a local user by entering the `username` command (CLI) or choosing Configuration > Device Management > Users/AAA > 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.

Support for administrator password policy when using the local database

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.

We introduced the following commands:
- `change-password`
- `password-policy lifetime`
- `password-policy minimum changes`
- `password-policy minimum-length`
- `password-policy minimum-lowercase`
- `password-policy minimum-uppercase`
- `password-policy minimum-numeric`
- `password-policy minimum-special`
- `password-policy authenticate enable`
- `clear configure password-policy`
- `show running-config password-policy`.

Support for SSH public key authentication

You can 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).

We introduced the following commands: `ssh authentication`.

PKF key format support is only in 9.1(2) and later.

Support for Diffie-Hellman Group 14 for the SSH Key Exchange

Support for Diffie-Hellman Group 14 for SSH Key Exchange was added. Formerly, only Group 1 was supported.

We introduced the following command: `ssh key-exchange`. 

Table 35-3  History for Management Access (continued)
Support for a maximum number of management sessions

- **Platform Releases**: 8.4(4.1), 9.1(2)
- **Description**: You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions.
  - We introduced the following commands: `quota management-session`, `show running-config quota management-session`, `show quota management-session`.

For the ASASM in multiple context mode, support for Telnet and virtual console authentication from the switch.

- **Platform Releases**: 8.5(1)
- **Description**: Although connecting to the ASASM from the switch in multiple context mode connects to the system execution space, you can configure authentication in the admin context to govern those connections.

AES-CTR encryption for SSH

- **Platform Releases**: 9.1(2)
- **Description**: The SSH server implementation in the ASA now supports AES-CTR mode encryption.

Improved SSH rekey interval

- **Description**: An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic.
  - We introduced the following command: `show ssh sessions detail`.

Improved one-time password authentication

- **Platform Releases**: 9.2(1)
- **Description**: Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once. The `auto-enable` option was added to the `aaa authorization exec` command.
  - We modified the following command: `aaa authorization exec`.

**Table 35-3  History for Management Access (continued)**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for a maximum number of management sessions</td>
<td>8.4(4.1), 9.1(2)</td>
<td>You can set the maximum number of simultaneous ASDM, SSH, and Telnet sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We introduced the following commands: <code>quota management-session</code>, <code>show running-config quota management-session</code>, <code>show quota management-session</code>.</td>
</tr>
<tr>
<td>For the ASASM in multiple context mode, support for Telnet and virtual console authentication from the switch.</td>
<td>8.5(1)</td>
<td>Although connecting to the ASASM from the switch in multiple context mode connects to the system execution space, you can configure authentication in the admin context to govern those connections.</td>
</tr>
<tr>
<td>AES-CTR encryption for SSH</td>
<td>9.1(2)</td>
<td>The SSH server implementation in the ASA now supports AES-CTR mode encryption.</td>
</tr>
<tr>
<td>Improved SSH rekey interval</td>
<td></td>
<td>An SSH connection is rekeyed after 60 minutes of connection time or 1 GB of data traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We introduced the following command: <code>show ssh sessions detail</code>.</td>
</tr>
<tr>
<td>Improved one-time password authentication</td>
<td>9.2(1)</td>
<td>Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once. The <code>auto-enable</code> option was added to the <code>aaa authorization exec</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following command: <code>aaa authorization exec</code>.</td>
</tr>
</tbody>
</table>
Software and Configurations

This chapter describes how to manage the Cisco ASA software and configurations.

- Upgrading the Software, page 36-1
- Managing Files, page 36-10
- Configuring the Images and Startup Configuration to Use, page 36-20
- Using the ROM Monitor to Load an Image, page 36-21
- Backing Up and Restoring Configurations or Other Files, page 36-24
- Downgrading Your Software, page 36-37
- Configuring Auto Update, page 36-39
- Feature History for Software and Configurations, page 36-46

Upgrading the Software

- Upgrade Path, page 36-1
- View Your Current Version, page 36-2
- Download the Software from Cisco.com, page 36-2
- Upgrade a Standalone Unit, page 36-2
- Upgrade a Failover Pair or ASA Cluster, page 36-4

Upgrade Path

See the following table for the upgrade path for your version. Some versions require an interim upgrade before you can upgrade to the latest version.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are no special requirements for Zero Downtime Upgrades for failover and ASA clustering with the following exception. Upgrading ASA clustering from 9.0(1) or 9.1(1): due to CSCue72961, hitless upgrading is not supported.</td>
</tr>
</tbody>
</table>
Chapter 36      Software and Configurations

Upgrading the Software

Configuration Migration

Depending on your current version, you might experience one or more configuration migrations when you upgrade. For example, when upgrading from 8.0 to 9.3, you will experience all of these migrations:

- 8.2—See the 8.2 release notes.
- 8.3—See the Cisco ASA 5500 Migration Guide to Version 8.3.
- 8.4—See the 8.4 upgrade guide.
- 9.0—See the 9.0 upgrade guide.

View Your Current Version

Use the `show version` command to verify the software version of your ASA.

Download the Software from Cisco.com

If you have a Cisco.com login, you can obtain the OS and ASDM images from the following website:
http://www.cisco.com/go/asa-software

This procedure assumes you put the images on a TFTP server, although other server types are supported.

Upgrade a Standalone Unit

This section describes how to install the ASDM and operating system (OS) images.

Procedure

This procedure uses TFTP. For FTP or HTTP, see the `copy` command.
Step 1  (If there is a configuration migration) Show the configuration on the terminal so that you can back up your configuration:

```
more system:running-config
```

Copy the output from this command, then paste the configuration in to a text file. For other methods of backing up, see the configuration guide.

Step 2  Copy the ASA software to the active unit flash memory:

```
copy tftp://server[/path]/asa_image_name {disk0:/ | disk1:/}[path/]asa_image_name
```

Example:

```
ciscoasa# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

For other methods than TFTP, see the `copy` command.

Step 3  Copy the ASDM image to the active unit flash memory:

```
copy tftp://server[/path]/asdm_image_name {disk0:/ | disk1:/}[path/]asdm_image_name
```

Example:

```
ciscoasa# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

Step 4  If you are not already in global configuration mode, access global configuration mode:

```
configure terminal
```

Step 5  Show the current boot images configured (up to 4):

```
show running-config boot system
```

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa914-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to Step 6 and Step 7.

Step 6  Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

```
no boot system {disk0:/ | disk1:/}[path/]asa_image_name
```

Example:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
```

Step 7  Set the ASA image to boot (the one you just uploaded):

```
boot system {disk0:/ | disk1:/}[path/]asa_image_name
```

Example:

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in Step 6.
Upgrading the Software

Chapter 36      Software and Configurations

Step 8    Set the ASDM image to use (the one you just uploaded):

```
asdm image (disk0:/ | disk1:/)[path/]asdm_image_name
```

Example:
```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 9    Save the new settings to the startup configuration:
```
write memory
```

Step 10   Reload the ASA:
```
reload
```

Upgrade a Failover Pair or ASA Cluster

- Upgrade an Active/Standby Failover Pair, page 36-4
- Upgrade an Active/Active Failover Pair, page 36-6
- Upgrade an ASA Cluster, page 36-8

Upgrade an Active/Standby Failover Pair

To upgrade the Active/Standby failover pair, perform the following steps.

Before You Begin
Perform these steps on the active unit.

Procedure

Step 1    (If there is a configuration migration) Show the configuration on the terminal so that you can back up your configuration:
```
more system:running-config
```

Example:
```
active# more system:running-config
```

Copy the output from this command, then paste the configuration in to a text file. For other methods of backing up, see the configuration guide.

Step 2    Copy the ASA software to the active unit flash memory:
```
copy tftp://server[/path]/asa_image_name (disk0:/ | disk1:/)[path/]asa_image_name
```

Example:
```
active# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

For other methods than TFTP, see the copy command.
**Step 3**  
Copy the software to the standby unit; be sure to specify the same path as for the active unit:

```plaintext
failover exec mate copy /noconfirm tftp://server[/path]/filename {disk0:/ | disk1:/}{path/}filename
```

Example:
```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

**Step 4**  
Copy the ASDM image to the active unit flash memory:

```plaintext
copy tftp://server[/path]/asdm_image_name {disk0:/ | disk1:/}{path/}asdm_image_name
```

Example:
```
active# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

**Step 5**  
Copy the ASDM image to the standby unit; be sure to specify the same path as for the active unit:

```plaintext
failover exec mate copy /noconfirm tftp://server[/path]/asdm_image_name {disk0:/ | disk1:/}{path/}asdm_image_name
```

Example:
```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

**Step 6**  
If you are not already in global configuration mode, access global configuration mode:

```plaintext
configure terminal
```

**Step 7**  
Show the current boot images configured (up to 4):

```plaintext
show running-config boot system
```

Example:
```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to **Step 8** and **Step 9**.

**Step 8**  
Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

```plaintext
no boot system {disk0:/ | disk1:/}{path/}asa_image_name
```

Example:
```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

**Step 9**  
Set the ASA image to boot (the one you just uploaded):

```plaintext
boot system {disk0:/ | disk1:/}{path/}asa_image_name
```

Example:
```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in **Step 8**.
**Upgrading the Software**

**Step 10** Set the ASDM image to use (the one you just uploaded):

```
asdm image (disk0:/ | disk1:/)[path/]asdm_image_name
```

Example:
```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

**Step 11** Save the new settings to the startup configuration:

```
write memory
```

**Step 12** Reload the standby unit to boot the new image:

```
failover reload-standby
```

Wait for the standby unit to finish loading. Use the `show failover` command to verify that the standby unit is in the Standby Ready state.

**Step 13** Force the active unit to fail over to the standby unit:

```
no failover active
```

**Step 14** Reload the former active unit (now the new standby unit):

```
reload
```

If you want to restore this unit to be active after it reloads, enter the `failover active` command.

---

**Upgrade an Active/Active Failover Pair**

To upgrade two units in an Active/Active failover configuration, perform the following steps.

**Before You Begin**
Perform these steps in the system execution space. Also perform these steps on the primary unit.

**Procedure**

**Step 1** (If there is a configuration migration) Show the configuration on the terminal so that you can back up your configuration:

```
moresystem:running-config
```

Copy the output from this command, then paste the configuration in to a text file. For other methods of backing up, see the configuration guide.

**Step 2** Copy the ASA software to the primary unit flash memory:

```
copy tftp://server[/path]/asa_image_name (disk0:/ | disk1:/)[path/]asa_image_name
```

Example:
```
primary# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

For other methods than TFTP, see the `copy` command.

**Step 3** Copy the software to the secondary unit; be sure to specify the same path as for the primary unit:
Upgrading the Software

**Step 4** Copy the ASDM image to the primary unit flash memory:

```
copy tftp://server[/path]/asdm_image_name {disk0:/ | disk1:/}[path/]asdm_image_name
```

Example:

```
primary# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

**Step 5** Copy the ASDM image to the secondary unit; be sure to specify the same path as for the active unit:

```
failover exec mate copy /noconfirm tftp://server[/path]/asdm_image_name {disk0:/ | disk1:/}[path/]asdm_image_name
```

Example:

```
primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

**Step 6** Make both failover groups active on the primary unit:

```
failover active group 1
failover active group 2
```

**Step 7** If you are not already in global configuration mode, access global configuration mode:

```
configure terminal
```

Example:

```
primary(config)# configure terminal
```

**Step 8** Show the current boot images configured (up to 4):

```
show running-config boot system
```

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to **Step 9** and **Step 10**.

**Step 9** Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

```
no boot system {disk0:/ | disk1:/}[path/]asa_image_name
```

Example:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

**Step 10** Set the ASA image to boot (the one you just uploaded):

```
boot system {disk0:/ | disk1:/}[path/]asa_image_name
```

Example:

```
ciscoasa(config)# boot system disk0:/asdm-731.bin
```
Example:

ciscoasa(config)# boot system disk0://asa931-smp-k8.bin

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in Step 9.

**Step 11**
Set the ASDM image to use (the one you just uploaded):

```
asdm image {disk0:/ | disk1:/}[path/]asdm_image_name
```

Example:

ciscoasa(config)# asdm image disk0:/asdm-731.bin

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

**Step 12**
Save the new settings to the startup configuration:

```
write memory
```

**Step 13**
Reload the secondary unit to boot the new image:

```
failover reload-standby
```

Wait for the secondary unit to finish loading. Use the `show failover` command to verify that both failover groups are in the Standby Ready state.

**Step 14**
Force both failover groups to become active on the secondary unit:

```
no failover active group 1
no failover active group 2
```

**Step 15**
Reload the primary unit:

```
reload
```

If the failover groups are configured with the `preempt` command, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with the `preempt` command, you can return them to active status on their designated units using the `failover active group` command.

---

**Upgrade an ASA Cluster**

To upgrade all units in an ASA cluster, perform the following steps on the master unit. For multiple context mode, perform these steps in the system execution space.

**Procedure**

**Step 1**
(If there is a configuration migration) Back up your configuration file:

```
more system:running-config
```

Copy the output from this command, then paste the configuration in to a text file. For other methods of backing up, see the general operations configuration guide.

**Step 2**
Copy the ASA software to all units in the cluster:
Step 3
Copy the ASDM image to all units in the cluster:
```
cluster exec copy /noconfirm tftp://server[/path]/asdm_image_name {disk0:/ | disk1:/}[path/]asdm_image_name
```
Example:
```
master# cluster exec copy /noconfirm tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```
For other methods than TFTP, see the `copy` command.

Step 4
If you are not already in global configuration mode, access global configuration mode:
```
configure terminal
```

Step 5
Show the current boot images configured (up to 4):
```
show running-config boot system
```
Example:
```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```
The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to Step 6 and Step 7.

Step 6
Remove any existing boot image configurations so that you can enter the new boot image as your first choice:
```
no boot system {disk0:/ | disk1:/}[path/]asa_image_name
```
Example:
```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

Step 7
Set the ASA image to boot (the one you just uploaded):
```
boot system {disk0:/ | disk1:/}[path/]asa_image_name
```
Example:
```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```
Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed in Step 6.

Step 8
Set the ASDM image to use (the one you just uploaded):
```
asdm image {disk0:/ | disk1:/}[path/]asdm_image_name
```
Example:
```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```
You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

**Step 9**
Save the new settings to the startup configuration:

```
write memory
```

**Step 10**
Reload each slave unit when you repeat this command for each unit name:

```
cluster exec unit slave-unit reload noconfirm
```

Example:

```
master# cluster exec unit unit2 reload noconfirm
```

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up (approximately 5 minutes) before reloading the next unit. To view member names, enter `cluster exec unit ?`, or enter the `show cluster info` command.

**Step 11**
Disable clustering on the master unit:

```
no enable
```

Wait for 5 minutes for a new master to be selected and traffic to stabilize. Do not enter `write memory`; when the master unit reloads, you want clustering to be enabled on it.

**Step 12**
Reload the master unit:

```
reload noconfirm
```

A new election takes place for a new master unit. When the former master unit rejoins the cluster, it will be a slave.

---

**Managing Files**

- Viewing Files in Flash Memory, page 36-10
- Deleting Files from Flash Memory, page 36-11
- Erasing the Flash File System, page 36-11
- Configuring File Access, page 36-11
- Copying a File to the ASA, page 36-16
- Copying a File to the Startup or Running Configuration, page 36-18

**Viewing Files in Flash Memory**

You can view files in flash memory and see information about files as follows:

- To view files in flash memory, enter the following command:
  
  ```
ciscoasa# dir [disk0: | disk1:]
  ```

  Enter `disk0:` for the internal flash memory. The `disk1:` keyword represents the external flash memory. The internal flash memory is the default.

  For example:
hostname# dir

Directory of disk0:/
500  -rw-  4958208  22:56:20 Nov 29 2004  cdisk.bin
2513  -rw-  4634  19:32:48 Sep 17 2004  first-backup
2788  -rw-  21601  20:51:46 Nov 23 2004  backup.cfg
2927  -rw-  8670632  20:42:48 Dec 08 2004  asdmfile.bin

- To view extended information about a specific file, enter the following command:
  hostname# show file information [path:]filename

  The default path is the root directory of the internal flash memory (disk0:/).
  For example:
  hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)

  The file size listed is for example only.

Deleting Files from Flash Memory

You can remove files from flash memory that you no longer need. To delete a file from flash memory, enter the following command:

hostname# delete disk0: filename

By default, the file is deleted from the current working directory if you do not specify a path. You may use wildcards when deleting files. You are prompted with the filename to delete, and then you must confirm the deletion.

Erasing the Flash File System

To erase the flash file system, perform the following steps:

1. Connect to the ASA console port according to the instructions in Access the ASA Services Module Console, page 2-2 or Access the Appliance Console, page 2-1.
2. Power off the ASA, then power it on.
3. During startup, press the Escape key when you are prompted to enter ROMMON mode.
4. Enter the erase command, which overwrites all files and erases the file system, including hidden system files.

   rommon #1> erase [disk0: | disk1: | flash:]

Configuring File Access

- Configuring the FTP Client Mode, page 36-12
Managing Files

- Configuring the ASA as a Secure Copy Server, page 36-12
- Customizing the ASA Secure Copy Client, page 36-13
- Configuring the ASA TFTP Client Path, page 36-15

Configuring the FTP Client Mode

The ASA can use FTP to upload or download image files or configuration files to or from an FTP server. In passive FTP, the client initiates both the control connection and the data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp mode passive</td>
<td>Sets the FTP mode to passive.</td>
</tr>
</tbody>
</table>

Example:
```plaintext
ciscoasa(config)# ftp mode passive
```

Configuring the ASA as a Secure Copy Server

You can enable the secure copy (SCP) server on the ASA. Only clients that are allowed to access the ASA using SSH can establish a secure copy connection.

Restrictions

- The server does not have directory support. The lack of directory support limits remote client access to the ASA internal files.
- The server does not support banners.
- The server does not support wildcards.

Prerequisites

- Enable SSH on the ASA according to Configure SSH Access, page 35-4.
- The ASA license must have the strong encryption (3DES/AES) license to support SSH Version 2 connections.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh scopy enable</td>
<td>Enables the SCP server.</td>
</tr>
</tbody>
</table>

Example:
```plaintext
ciscoasa(config)# ssh scopy enable
```
Example

From a client on the external host, perform an SCP file transfer. For example, in Linux enter the following command:

```bash
scp -v -pw password source_filename username@asa_address:(disk0|disk1):/dest_filename
```

The `-v` is for verbose, and if `-pw` is not specified, you will be prompted for a password.

Customizing the ASA Secure Copy Client

You can copy files to and from the ASA using the on-board SCP client (see Copying a File to the ASA, page 36-16). This section lets you customize the SCP client operation.

Prerequisites

For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the `changeto system` command.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>[no] ssh stricthostkeycheck</td>
<td>Enables or disables SSH host key checking. By default, this option is enabled. When this option is enabled, you are prompted to accept or reject the host key if it is not already stored on the ASA. When this option is disabled, the ASA accepts the host key automatically if it was not stored before.</td>
</tr>
</tbody>
</table>

**Example:**

ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is
c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?
Address or name of remote host [10.86.95.9]?
Destination username [cisco]?
Destination password []? cisco123
Destination filename [x]?

<table>
<thead>
<tr>
<th>Step 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh pubkey-chain</td>
<td>The ASA stores the SSH host key for each SCP server to which it connects. You can manually add or delete servers and their keys from the ASA database if desired.</td>
</tr>
</tbody>
</table>

**Example:**
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key. End with the word "exit" on a line by itself
63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
server 10.7.8.9
key-hash sha256
0e:d2:86:12
Examples

The following example adds an already hashed host key for the server at 10.86.94.170:

ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256

The following example adds a host string key for the server at 10.7.8.9:

ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself


ciscoasa(config-ssh-pubkey-server-string)# exit

Configuring the ASA TFTP Client Path

TFTP is a simple client/server file transfer protocol, which is described in RFC 783 and RFC 1350 Rev. 2. You can configure the ASA as a TFTP client so that it can copy files to or from a TFTP server (see Copying a File to the ASA, page 36-16 and Backing Up and Restoring Configurations or Other Files, page 36-24. In this way, you can back up and propagate configuration files to multiple ASAs.

This section lets you predefine the path to a TFTP server so you do not need to enter it in commands such as copy and configure net.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>tftp-server</td>
<td>Predefines the TFTP server address and filename for use with configure net and copy commands. You can override the filename when you enter the command; for example, when you use the copy command, you can take advantage of the predefined TFTP server address but still enter any filename at the interactive prompts. For the copy command, enter tftp: to use the tftp-server value instead of tftp://url.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>interface_name</td>
<td></td>
</tr>
<tr>
<td>server_ip</td>
<td></td>
</tr>
<tr>
<td>filename</td>
<td></td>
</tr>
</tbody>
</table>

Example:

ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]? 

Source filename
[files/config1.cfg]? config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
Copying a File to the ASA

This section describes how to copy the application image, ASDM software, a configuration file, or any other file that needs to be downloaded to internal or external flash memory from a TFTP, FTP, SMB, HTTP, HTTPS, or SCP server.

Guidelines

- For the IPS SSP software module, before you download the IPS software to disk0, make sure at least 50% of the flash memory is free. When you install IPS, IPS reserves 50% of the internal flash memory for its file system.
- You cannot have two files with the same name but with different letter case in the same directory in flash memory. For example, if you attempt to download the file, Config.cfg, to a location that contains the file, config.cfg, you receive the following error message:

  %Error opening disk0:/Config.cfg (File exists).

- For information about installing the Cisco SSL VPN client, see the Cisco AnyConnect VPN Client Administrator Guide. For information about installing Cisco Secure Desktop on the ASA, see the Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators.
- To configure the ASA to use a specific application image or ASDM image if you have more than one installed, or have installed them in external flash memory, see Configuring the Images and Startup Configuration to Use, page 36-20.
- For multiple context mode, you must be in the system execution space.
### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`copy [noconfirm] tftp://server[/path]/src_filename {disk0</td>
<td>disk1}:[/path/]dest_filename`</td>
</tr>
</tbody>
</table>

**Example:**
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?
Source filename [files/context1.cfg]?
Destination filename [context1.cfg]?
Cryptos checksum: db8ba196 9ad189a8 7f5f501f 1bec469b
11143 bytes copied in 5.710 secs (2228 bytes/sec)

| `copy [noconfirm] ftp://[user[:password]@]server[/path]/src_filename {disk0|disk1}:[/path/]dest_filename` | Copies from an FTP server. |

**Example:**
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?
Source username [jcrichton]?
Source password [aeryn]?
Source filename [files/context1.cfg]?
Destination filename [contexts/context1.cfg]?
Cryptos checksum: db8ba196 9ad189a8 7f5f501f 1bec469b
11143 bytes copied in 5.710 secs (2228 bytes/sec)

| `copy [noconfirm] http[s]://[user[:password]@]server[:port][/path]/src_filename {disk0|disk1}:[/path/dest_filename]` | Copies from an HTTP(S) server. |

**Example:**
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?
Source username [asun]?
Source password [john]?
Source filename [files/moya.cfg]?
Destination filename [contexts/moya.cfg]?
Cryptos checksum: db8ba196 9ad189a8 7f5f501f 1bec469b
11143 bytes copied in 5.710 secs (2228 bytes/sec)
### Managing Files

#### Copying a File to the Startup or Running Configuration

You can download a text file to the running or startup configuration from a TFTP, FTP, SMB, HTTP(S), or SCP server, or from the flash memory.

To configure the ASA to use a specific configuration as the startup configuration, see Configuring the Images and Startup Configuration to Use, page 36-20.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy [[noconfirm]] smb://[[user[:password]@[server[/path]/src_filename](({disk0</td>
<td>disk1}):/[path])]dest_filename]</td>
</tr>
<tr>
<td>copy [[noconfirm]] scp://[[user[:password]@[server[/path]/src_filename;int=interface_name](({disk0</td>
<td>disk1}):/[path)]dest_filename]</td>
</tr>
</tbody>
</table>

#### Example:

**copy to SMB server:**

```bash
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml
```

Crytopchecksum: db8ba196 9ad189a8 7f5f501f 1bec469b

!!!!!!!!!!!

11143 bytes copied in 5.710 secs (2228 bytes/sec)

**copy to SCP server:**

```bash
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg
```

Please use the following commands to add the hash key to the configuration:

```bash
ssh pubkey-chain
server 10.86.94.170
key-hash sha256
```


Password: <type in password>

!!!!!!!

6006 bytes copied in 8.160 secs (750 bytes/sec)
Guidelines

When you copy a configuration to the running configuration, you merge the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.

Detailed Steps

To copy a file to the startup configuration or running configuration, enter one of the following commands for the appropriate download server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`copy [noconfirm] tftp://server[/path]/src_filename {startup-config</td>
<td>running-config}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config</code></td>
<td></td>
</tr>
<tr>
<td>`copy [noconfirm] ftp://[user[:password]@]server[/path]/src_filename {startup-config</td>
<td>running-config}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config</code></td>
<td></td>
</tr>
<tr>
<td>`copy [noconfirm] http(s)://[user[:password]@]server[:port][/path]/src_filename {startup-config</td>
<td>running-config}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config</code></td>
<td></td>
</tr>
<tr>
<td>`copy [noconfirm] smb://[user[:password]@]server[/path]/src_filename {startup-config</td>
<td>running-config}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config</code></td>
<td></td>
</tr>
<tr>
<td>`copy [noconfirm] scp://[user[:password]@]server[/path]/src_filename[;int=interface_name] {startup-config</td>
<td>running-config}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

Examples

For example, to copy the configuration from a TFTP server, enter the following command:

`ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config`
To copy the configuration from an FTP server, enter the following command:
```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```
To copy the configuration from an HTTP server, enter the following command:
```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

## Configuring the Images and Startup Configuration to Use

If you have more than one ASA or ASDM image, you should specify the image that you want to boot. If you do not set the image, the default boot image is used, and that image may not be the one intended. For the startup configuration, you can optionally specify a configuration file.

### Default Settings

#### ASA Image
- Physical ASA—Boots the first application image that it finds in internal flash memory.
- ASAv—Boots the image in the read-only boot:/ partition that was created when you first deployed. You can upgrade the image in flash memory and configure the ASAv to boot from that image. Note that if you later clear your configuration (`clear configure all`), then the ASAv will revert to loading the original deployment image.

#### ASDM Image
All ASAs—Boots the first ASDM image that it finds in internal flash memory, or if one does not exist in this location, then in external flash memory.

#### Startup Configuration
By default, the ASA boots from a startup configuration that is a hidden file.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>boot system <strong>url</strong></td>
<td>Sets the ASA boot image location. The URL can be:</td>
</tr>
<tr>
<td></td>
<td>- `{disk0:/}</td>
</tr>
<tr>
<td></td>
<td>- <code>tftp://[user[:password]@]server[:port]/[path/]filename</code></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config)# boot system disk0:/images/asa921.bin</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>asdm image `{disk0:/}</td>
<td>Sets the ASDM image to boot. If you do not specify the image to</td>
</tr>
<tr>
<td>disk1:/}[path/]filename</td>
<td>boot, even if you have only one image installed, then the ASA</td>
</tr>
<tr>
<td></td>
<td>inserts the <code>asdm image</code> command into the running configuration.</td>
</tr>
<tr>
<td></td>
<td>To avoid problems with Auto Update (if configured), and to avoid</td>
</tr>
<tr>
<td></td>
<td>the image search at each startup, you should specify the ASDM</td>
</tr>
<tr>
<td></td>
<td>image that you want to boot in the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config)# asdm image disk0:/images/asdm721.bin</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>boot config `{disk0:/}</td>
<td>Sets the startup configuration to be a known file instead of the</td>
</tr>
<tr>
<td>disk1:/}[path/]filename</td>
<td>default hidden file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ciscoasa(config)# boot config disk0:/configs/startup1.cfg</td>
<td></td>
</tr>
</tbody>
</table>

Using the ROM Monitor to Load an Image

- Using ROM Monitor for the ASA 5500-X Series, page 36-22
- Using the ROM Monitor for the ASASM, page 36-23
Using ROM Monitor for the ASA 5500-X Series

To load a software image to an ASA from the ROM monitor mode using TFTP, perform the following steps:

**Step 1** Connect to the ASA console port according to the instructions in Access the Appliance Console, page 2-1.

**Step 2** Power off the ASA, then power it on.

**Step 3** During startup, press the **Escape** key when you are prompted to enter ROMMON mode.

**Step 4** In ROMMON mode, define the interface settings to the ASA, including the IP address, TFTP server address, gateway address, software image file, and port, as follows:

- **Note** For the ASA 5506-X, you do not need to include the PORT=Ethernet0/0 entry. Only the management port is available.

  ```
  rommon #1> ADDRESS=10.132.44.177
  rommon #2> SERVER=10.129.0.30
  rommon #3> GATEWAY=10.132.44.1
  rommon #4> IMAGE=f1/asa800-232-k8.bin
  rommon #5> PORT=Ethernet0/0
  Ethernet0/0
  Link is UP
  MAC Address: 0012.d949.15b8
  
  **Note** Be sure that the connection to the network already exists.
  ```

**Step 5** To validate your settings, enter the **set** command.

  ```
  rommon #6> set
  ROMMON Variable Settings:
  ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa840-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
  ```

**Step 6** Ping the TFTP server by entering the **ping server** command.

  ```
  rommon #7> ping server
  Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:
  
  Success rate is 100 percent (20/20)
  ```

**Step 7** Load the software image by entering the **tftp** command.

  ```
  rommon #8> tftp
  ROMMON Variable Settings:
  ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  ```
Chapter 36  Software and Configurations

Using the ROM Monitor to Load an Image

VLAN=untagged
IMAGE=f1/asa840-232-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20
tftp f1/asa840-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2011

Loading...N

After the software image is successfully loaded, the ASA automatically exits ROMMON mode.

Step 8
To verify that the correct software image has been loaded into the ASA, check the version in the ASA by entering the following command:
ciscoasa# show version

Using the ROM Monitor for the ASASM

To load a software image to an ASASM from the ROM monitor mode using TFTP, perform the following steps:

Step 1
Connect to the ASA console port according to the instructions in Access the ASA Services Module Console, page 2-2.

Step 2
Make sure that you reload the ASASM image.

Step 3
During startup, press the Escape key when you are prompted to enter ROMMON mode.

Step 4
In ROMMOM mode, define the interface settings to the ASASM, including the IP address, TFTP server address, gateway address, software image file, port, and VLAN, as follows:

rommon #1> ADDRESS=172.16.145.149
rommon #2> SERVER=172.16.171.125
rommon #3> GATEWAY=172.16.145.129
rommon #4> IMAGE=f1/asa851-smp-k8.bin
rommon #5> PORT=Data0
rommon #6> VLAN=1
Data0
Link is UP
MAC Address: 0012.d949.15b8

Note
Be sure that the connection to the network already exists.

Step 5
To validate your settings, enter the set command.

rommon #7> set
ROMMON Variable Settings:
ADDRESS=172.16.145.149
SERVER=172.16.171.125
GATEWAY=172.16.145.129
PORT=Data0
VLAN=1
Step 6  Ping the TFTP server by entering the ping server command.

    rommon #8> ping server
    Sending 20, 100-byte ICMP Echoes to server 172.16.171.125, timeout is 2 seconds:
    Success rate is 100 percent (20/20)

Step 7  Load the software image by entering the tftp command.

    rommon #9> tftp
    Clearing EOBC receive queue ...
    cmostime_set = 1
    ROMMON Variable Settings:
    ADDRESS=172.16.145.149
    SERVER=172.16.171.125
    GATEWAY=172.16.145.129
    PORT=Data0
    VLAN=1
    IMAGE=f1/asa851-smp-k8.bin
    CONFIG=
    LINKTIMEOUT=20
    PKTTIMEOUT=2
    RETRY=20

    tftp f1/asa851-smp-k8.bin@172.16.171.125 via 172.16.145.129
    Starting download. Press ESC to abort.

After the software image is successfully loaded, the ASASM automatically exits ROMMON mode.

Note  You must download the image to the system flash separately after ROMMON boot is complete; booting the module into ROMMON mode does not preserve the system image across reloads.

Step 8  To verify that the correct software image has been loaded into the ASASM, check the version by entering the following command:

    hostname# show version

---

**Backing Up and Restoring Configurations or Other Files**

We recommend that you make regular backups of your configuration and other system files to guard against system failure.

- Perform a Complete System Backup or Restoration, page 36-25
- Backing up the Single Mode Configuration or Multiple Mode System Configuration, page 36-29
- Backing Up a Context Configuration or Other File in Flash Memory, page 36-29
- Backing Up a Context Configuration within a Context, page 36-30
- Copying the Configuration from the Terminal Display, page 36-31
Perform a Complete System Backup or Restoration

These procedures describe how to back up and restore configurations and images to a tar.gz file and transfer it to your local computer.

- Before You Begin, page 36-25
- Back Up the System, page 36-26
- Restore the Backup, page 36-27

Before You Begin

- You should have at least 300 MB of disk space available at the backup or restore location before you start a backup or restore.
- If you make any configuration changes during or after a backup, those changes will not be included in the backup. If you change a configuration after making the backup, then perform a restore, this configuration change will be overwritten. As a result, the ASA might behave differently.
- You can start only one backup or restore at a time.
- You can only restore a configuration to the same ASA version as when you performed the original backup. You cannot use the restore tool to migrate a configuration from one ASA version to another. If a configuration migration is required, the ASA automatically upgrades the resident startup configuration when it loads the new ASA OS.
- If you use clustering, you can only back up or restore the startup-configuration, running-configuration, and identity certificates. You must create and restore a backup separately for each unit.
- If you use failover, you must create and restore a backup separately for the active and standby units.
- If you set a master passphrase for the ASA, then you need that master passphrase to restore the backup configuration that you create with this procedure. If you do not know the master passphrase for the ASA, see Configure the Master Passphrase, page 14-10 to learn how to reset it before continuing with the backup.
- If you import PKCS12 data (with the crypto ca trustpoint command) and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint. Because of this limitation, if you specify a different name for the trustpoint and its key pair after you have restored an ASDM configuration, the startup configuration will be the same as the original configuration, but the running configuration will include a different key pair name. This means that if you use different names for the key pair and trustpoint, you cannot restore the original configuration. To work around this issue, make sure that you use the same name for the trustpoint and its key pair.
- You cannot back up using the CLI and restore using ASDM, or vice versa.
- Each backup file includes the following content:
  - Running-configuration
  - Startup-configuration
  - All security images
    - Cisco Secure Desktop and Host Scan images
Cisco Secure Desktop and Host Scan settings
AnyConnect (SVC) client images and profiles
AnyConnect (SVC) customizations and transforms
  - Identity certificates (includes RSA key pairs tied to identity certificates; excludes standalone keys)
  - VPN pre-shared keys
  - SSL VPN configurations
  - Application Profile Custom Framework (APCF)
  - Bookmarks
  - Customizations
  - Dynamic Access Policy (DAP)
  - Plug-ins
  - Pre-fill scripts for connection profiles
  - Proxy Auto-config
  - Translation table
  - Web content
  - Version information

Back Up the System

This procedure describes how to perform a complete system backup.

Procedure

Step 1 Back up the system.

```
backup [/noconfirm] [context name] [cert-passphrase value] [location path]
```

Example:

ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]? 

In multiple context mode from the system execution space, enter the `context` keyword to backup the specified context files.

During the backup of VPN certificates and preshared keys, a secret key identified by the `cert-passphrase` keyword is required to encode the certificates. You must provide a passphrase to be used for encoding and decoding the certificates in PKCS12 format. The backup only includes RSA key pairs tied to the certificates and excludes any standalone certificates.

The backup location can be a local disk or a remote URL. If you do not provide a location, the following default names are used:

- Single mode—`disk0:hostname.backup.timestamp.tar.gz`
- Multiple mode—`disk0:hostname.context-ctx-name.backup.timestamp.tar.gz`

Step 2 Follow the prompts:

Example:
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup...
Backing up [ASA version]  ... Done!
Backing up [Running Config] ... Done!
Backing up [Startup Config] ... Done!

Enter a passphrase to encrypt identity certificates. The default is cisco. You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] ... Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file is used to restore to a device with a different master passphrase, you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] ... Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] ... Done!
Backing up [SSL VPN Configurations: Bookmarks] ... Done!
Backing up [SSL VPN Configurations: Customization] ... Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] ... Done!
Backing up [SSL VPN Configurations: Plug-in] ... Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] ... Done!
Backing up [SSL VPN Configurations: Proxy auto-config] ... Done!
Backing up [SSL VPN Configurations: Translation table] ... Done!
Backing up [SSL VPN Configurations: Web Content] ... Done!
Backing up [Anyconnect(SVC) client images and profiles] ... Done!
Backing up [Anyconnect(SVC) customizations and transforms] ... Done!
Backing up [Cisco Secure Desktop and Host Scan Images] ... Done!
Backing up [UC-IMC tickets] ... Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!

Restore the Backup

You can specify configurations and images to restore from a tar.gz file on your local computer.

Procedure

Step 1  Restore the system from the backup file.

    restore [/noconfirm] [context name] [cert-passphrase value] [location path]

Example:

ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Step 2  Follow the prompts:

Example:

ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup directory ... Done!
Warning: The ASA version of the device is not the same as the backup version, some configurations might not work after restore!

Do you want to continue? [confirm] y

Begin restore ...

IMPORTANT: This backup configuration uses master passphrase encryption. Master passphrase is required to restore running configuration, startup configuration and VPN pre-shared keys.

Backing up [VPN Pre-shared keys] ... Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] ... Done!
Backing up [SSL VPN Configurations: Bookmarks] ... Done!
Backing up [SSL VPN Configurations: Customization] ... Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] ... Done!
Backing up [SSL VPN Configurations: Plug-in] ... Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] ... Done!
Backing up [SSL VPN Configurations: Proxy auto-config] ... Done!
Backing up [SSL VPN Configurations: Translation table] ... Done!
Backing up [SSL VPN Configurations: Web Content] ... Done!
Backing up [Anyconnect(SVC) client images and profiles] ... Done!
Backing up [Anyconnect(SVC) customizations and transforms] ... Done!
Backing up [Cisco Secure Desktop and Host Scan images] ... Done!
Backing up [UC-IME tickets] ... Done!

Restoring [Running Configuration]

Following messages are as a result of applying the backup running-configuration to this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information ...
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside, the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside, the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations. Do not overwrite configuration file if you want to preserve the old http- and https-proxy configurations.

Cryptochecksum (changed): 9823c2c ccb31dc3 e51acf88 19f04e28
Done!

Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates. The default is cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates. Using the default value: cisco. If the passphrase is not correct, certificates will not be restored.

Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully.
Done!

Cleaning up ... Done!

Restore finished!
Backing up the Single Mode Configuration or Multiple Mode System Configuration

In single context mode or from the system configuration in multiple mode, you can copy the startup configuration or running configuration to an external server or to the local flash memory.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`copy [/noconfirm] {startup-config</td>
<td>running-config} tftp://server[/path]/dst_filename`</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg</code></td>
<td></td>
</tr>
<tr>
<td>`copy [/noconfirm] {startup-config</td>
<td>running-config} ftp://[user:password]@server[/path]/dst_filename`</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg</code></td>
<td></td>
</tr>
<tr>
<td>`copy [/noconfirm] {startup-config</td>
<td>running-config} smb://[user:password]@server[/path]/dst_filename`</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg</code></td>
<td></td>
</tr>
<tr>
<td>`copy [/noconfirm] {startup-config</td>
<td>running-config} scp://[user:password]@server[/path]/dst_filename;int=interface_name`</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa# copy startup-config scp://pilot:moya@10.86.94.170/new-startup.cfg</code></td>
<td></td>
</tr>
<tr>
<td>`copy [/noconfirm] {startup-config</td>
<td>running-config} {disk0</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;<code>ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg</code></td>
<td></td>
</tr>
</tbody>
</table>

**Backing Up a Context Configuration or Other File in Flash Memory**

Copy context configurations or other files that are on the local flash memory by entering one of the following commands in the system execution space.
## Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`copy [/noconfirm] {disk0</td>
<td>disk1}:[/path/]src_filename<code>&lt;br&gt;</code>tftp://server[/path]/dst_filename`</td>
</tr>
<tr>
<td>`copy [/noconfirm] {disk0</td>
<td>disk1}:[/path/]src_filename<code>&lt;br&gt;</code>ftp://[user[:password]@]server[/path]/dst_filename`</td>
</tr>
<tr>
<td>`copy [/noconfirm] {disk0</td>
<td>disk1}:[/path/]src_filename<code>&lt;br&gt;</code>smb://[user[:password]@]server[/path]/dst_filename`</td>
</tr>
<tr>
<td><code>copy /noconfirm copy disk0:/asdm.bin</code>&lt;br&gt;<code>smb://chiana:dargo@10.1.1.67/asdm.bin</code></td>
<td>Copies from flash to SCP server. The ;int=interface option bypasses the route lookup and always uses the specified interface to reach the SCP server.</td>
</tr>
<tr>
<td>`copy {disk0</td>
<td>disk1}:[/path/]src_filename<code>&lt;br&gt;</code>{disk0</td>
</tr>
</tbody>
</table>

## Backing Up a Context Configuration within a Context

In multiple context mode, from within a context, you can perform the following backups:

- To copy the running configuration to the startup configuration server (connected to the admin context), enter the following command:
  ```
ciscoasa/contexta# copy running-config startup-config
  ```

- To copy the running configuration to a TFTP server connected to the context network, enter the following command:
  ```
ciscoasa/contexta# copy running-config tftp://server[/path]/filename
  ```
Copying the Configuration from the Terminal Display

To print the configuration to the terminal, enter the following command:

```bash
CiscoASA# show running-config
```

Copy the output from this command, and then paste the configuration into a text file.

Backing Up Additional Files Using the Export and Import Commands

Additional files essential to your configuration might include the following:

- Files that you import using the `import webvpn` command. Currently, these files include customizations, URL lists, web content, plug-ins, and language translations.
- DAP policies (dap.xml).
- CSD configurations (data.xml).
- Digital keys and certificates.
- Local CA user database and certificate status files.

The CLI lets you back up and restore individual elements of your configuration using the `export` and `import` commands.

To back up these files, for example, those files that you imported with the `import webvpn` command or certificates, perform the following steps:

**Step 1** Run the applicable `show` command(s) as follows:

```bash
CiscoASA# show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

**Step 2** Run the `export` command for the file that you want to back up (in this example, the rdp file):

```bash
CiscoASA# export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

Using a Script to Back Up and Restore Files

You can use a script to back up and restore the configuration files on your ASA, including all extensions that you import via the `import webvpn` CLI, the CSD configuration XML files, and the DAP configuration XML file. For security reasons, we do not recommend that you perform automated backups of digital keys and certificates or the local CA key.

This section provides instructions for doing so and includes a sample script that you can use as is or modify as your environment requires. The sample script is specific to a Linux system. To use it for a Microsoft Windows system, you need to modify it using the logic of the sample.
The existing CLI lets you back up and restore individual files using the `copy`, `export`, and `import` commands. It does not, however, have a facility that lets you back up all ASA configuration files in one operation. Running the script facilitates the use of multiple CLIs.

- Prerequisites, page 36-32
- Running the Script, page 36-32
- Sample Script, page 36-32

**Prerequisites**

To use a script to back up and restore an ASA configuration, first perform the following tasks:

- Install Perl with an Expect module.
- Install an SSH client that can reach the ASA.
- Install a TFTP server to send files from the ASA to the backup site.

Another option is to use a commercially available tool. You can put the logic of this script into such a tool.

**Running the Script**

To run a backup-and-restore script, perform the following steps:

1. Download or cut-and-paste the script file to any location on your system.
2. At the command line, enter `Perl scriptname`, where `scriptname` is the name of the script file.
3. Press Enter.
4. The system prompts you for values for each option. Alternatively, you can enter values for the options when you enter the `Perl scriptname` command before you press Enter. Either way, the script requires that you enter a value for each option.
5. The script starts running, printing out the commands that it issues, which provides you with a record of the CLIs. You can use these CLIs for a later restore, which is particularly useful if you want to restore only one or two files.

**Sample Script**

```bash
#!/usr/bin/perl
#Function: Backup/restore configuration/extensions to/from a TFTP server.
#Description: The objective of this script is to show how to back up configurations/extensions before the backup/restore command is developed.
# It currently backs up the running configuration, all extensions imported via "import webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
# -h: ASA hostname or IP address
# -u: User name to log in via SSH
# -w: Password to log in via SSH
# -e: The Enable password on the security appliance
```
# -p: Global configuration mode prompt
# -s: Host name or IP address of the TFTP server to store the configurations
# -r: Restore with an argument that specifies the file name. This file is produced
during backup.
# If you don't enter an option, the script will prompt for it prior to backup.
# Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

# global variables
%options=();
$restore = 0; # does backup by default
$restore_file = '';  
$asa = '';  
$storage = '';  
$user = '';  
$password = '';  
$enable = '';  
$prompt = '';  
$date = `date +%F' ;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:","\%options");
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
do restore($exp,$restore_file);
}
else {
$restore_file = "$prompt-restore-$date.cli";
open(OUT,">$restore_file") or die "Can't open $restore_file\n";
do running_config($exp);
do lang_trans($exp);
do customization($exp);
do plugin($exp);
do url_list($exp);
do webcontent($exp);
do dap($exp);
do csd($exp);
close(OUT);
}
do finish($exp);

sub enable {
$obj = shift;
$obj->send("enable\n");
unless ($obj->expect(15, 'Password:')) {
print "timed out waiting for Password:\n";
}
$obj->send("$enable\n");
unless ($obj->expect(15, "$prompt#")) {
print "timed out waiting for $prompt#\n";
}
}

sub lang_trans {
$obj = shift;
$obj->clear_accum();
$obj->send("show import webvpn translation-table\n");
Backing Up and Restoring Configurations or Other Files

```perl
# Backing up configuration files
$obj->expect(15, "$prompt# ");
$output = $obj->before();
@items = split(/\n+/, $output);

for (@items) {
    s/\s+/;
    s/\s+$/;
    next if /show import/ or /Translation Tables/;
    next unless (/^\s+\s+/);  
    ($lang, $transtable) = split(/\s+/,$_);
    $cli = "export webvpn translation-table $transtable language $lang
    $storage/$prompt-$date-$transtable-$lang.po";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$ocli\n";
    print OUT "$ocli\n";
    $obj->send("$ocli\n");
    $obj->expect(15, "$prompt# ");
}

sub running_config {  
    $obj = shift;
    $obj->clear_accum();
    $cli = "copy /noconfirm running-config $storage/$prompt-$date.cfg";
    print "$cli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt# ");
}

sub customization {  
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn customization\n");
    $obj->expect(15, "$prompt# ");
    $output = $obj->before();
    @items = split(/\n+/, $output); 
    for (@items) {
        chop;
        next if /^Template/ or /show import/ or /^\s+$/;
        $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
        $ocli = $cli;
        $ocli =~ s/^export/import/;
        print "$ocli\n";
        print OUT "$ocli\n";
        $obj->send("$ocli\n");
        $obj->expect(15, "$prompt# ");
    }
}

sub plugin {  
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn plug-in\n");
    $obj->expect(15, "$prompt# ");
    $output = $obj->before();
    @items = split(/\n+/, $output); 
    for (@items) {
        chop;
        next if /^Template/ or /show import/ or /^\s+$/;
        $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
```
$ocli = $cli;
$ocli =~ s/^export/import/;
print "$ocli\n";
print OUT "$ocli\n";
$obj->send("$ocli\n");
$obj->expect(15, "$prompt#" );
}

sub url_list {
$obj = shift;
$obj->clear_accum();
$obj->send("show import webvpn url-list\n");
$obj->expect(15, "$prompt#" );
$output = $obj->before();
@items = split(/\n+/, $output);
for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
    $cli="export webvpn url-list $_ $storage/$prompt-$date-url-list-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$ocli\n";
    print OUT "$ocli\n";
    $obj->send("$ocli\n");
    $obj->expect(15, "$prompt#" );
}

sub dap {
$obj = shift;
$obj->clear_accum();
$obj->send("dir dap.xml\n");
$obj->expect(15, "$prompt#" );
$output = $obj->before();
return 0 if($output =~ /Error/);
(cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
$ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
print "$cli\n";
print OUT "$ocli\n";
$obj->send("$ocli\n");
$obj->expect(15, "$prompt#" );
}

sub csd {
$obj = shift;
$obj->clear_accum();
$obj->send("dir sdesktop\n");
$obj->expect(15, "$prompt#" );
$output = $obj->before();
return 0 if($output =~ /Error/);
(cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
$ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
print "$cli\n";
print OUT "$ocli\n";
$obj->send("$ocli\n");
$obj->expect(15, "$prompt#" );
}
sub webcontent {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn webcontent\n");
    $obj->expect(15, "$prompt# ");
    $output = $obj->before();
    @items = split(/\n\+/, $output);
    for (@items) {
        s/^\s+//;
        s/\s+$//;
        next if /show import/ or /No custom/;
        next unless (/^\s+\s+.+$/);
        ($url, $type) = split(/\s+\s+/, $_);
        $turl = $url;
        $turl =~ s/\+/-/;
        $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
        $ocli = $cli;
        $ocli =~ s/export/import/;
        print "$ocli\n";
        print OUT "$ocli\n";
        $obj->send("$ocli\n");
        $obj->expect(15, "$prompt# ");
    }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }
    $obj->send("$password\n");
    unless ($obj->expect(15, "$prompt> ") ) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";
}

sub restore {
    $obj = shift;
    my $file = shift;
    my $output;
    open(IN, "$file") or die "can't open $file\n";
    while (<IN>) {
        $obj->send("S_*");
        $obj->expect(15, "$prompt# ");
        $output = $obj->before();
        print "$output\n";
    }
    close(IN);
}
Downgrading Your Software

When you upgrade to Version 8.3, your configuration is migrated. The old configuration is automatically stored in flash memory. For example, when you upgrade from Version 8.2(1) to 8.3(1), the old 8.2(1) configuration is stored in flash memory in a file called 8_2_1_0_startupcfg.sav.
Downgrading Your Software

Chapter 36      Software and Configurations

Note

You must manually restore the old configuration before downgrading.

This section describes how to downgrade.

- Information About Activation Key Compatibility, page 36-38
- Performing the Downgrade, page 36-38

Information About Activation Key Compatibility

Your activation key remains compatible if you upgrade to the latest version from any previous version. However, you might have issues if you want to maintain downgrade capability:

- Downgrading to Version 8.1 or earlier versions—After you upgrade, if you activate additional feature licenses that were introduced before 8.2, the activation key continues to be compatible with earlier versions if you downgrade. However, if you activate feature licenses that were introduced in Version 8.2 or later versions, the activation key is not backwards compatible. If you have an incompatible license key, see the following guidelines:
  - If you previously entered an activation key in an earlier version, the ASA uses that key (without any of the new licenses you activated in Version 8.2 or later versions).
  - If you have a new system and do not have an earlier activation key, you need to request a new activation key compatible with the earlier version.

- Downgrading to Version 8.2 or earlier versions—Version 8.3 introduced more robust time-based key usage as well as failover license changes:
  - If you have more than one time-based activation key active, when you downgrade, only the most recently activated time-based key can be active. Any other keys are made inactive.
  - If you have mismatched licenses on a failover pair, downgrading will disable failover. Even if the keys are matching, the license used will no longer be a combined license.

Performing the Downgrade

To downgrade from Version 8.3, perform the following steps:

Detailed Steps

Step 1

Enter the following command:

ciscoasa(config)# downgrade [/noconfirm] old_image_url old_config_url [activation-key old_key]

Where the /noconfirm option downgrades without prompting. The image_url is the path to the old image on disk0, disk1, tftp, ftp, or smb. The old_config_url is the path to the saved, premigration configuration (by default, this configuration was saved on disk0). If you need to revert to a pre-8.3 activation key, you can enter the old activation key.

This command is a shortcut for completing the following functions:

1. Clearing the boot image configuration (clear configure boot).
2. Setting the boot image to be the old image (boot system).
3. (Optional) Entering a new activation key (activation-key).
4. Saving the running configuration to startup (write memory). This action sets the BOOT environment variable to the old image, so when you reload, the old image is loaded.
5. Copying the old configuration to the startup configuration (copy old_config_url startup-config).
6. Reloading (reload).

For example:
```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

---

**Configuring Auto Update**

- Information About Auto Update, page 36-39
- Guidelines and Limitations, page 36-42
- Configuring Communication with an Auto Update Server, page 36-42
- Configuring Client Updates as an Auto Update Server, page 36-44
- Viewing Auto Update Status, page 36-45

**Information About Auto Update**

Auto Update is a protocol specification that allows an Auto Update Server to download configurations and software images to many ASAs and can provide basic monitoring of the ASAs from a central location.

- Auto Update Client or Server, page 36-39
- Auto Update Benefits, page 36-39
- Auto Update Server Support in Failover Configurations, page 36-40

**Auto Update Client or Server**

The ASA can be configured as either a client or a server. As an Auto Update client, it periodically polls the Auto Update Server for updates to software images and configuration files. As an Auto Update Server, it issues updates for ASAs configured as Auto Update clients.

**Auto Update Benefits**

Auto Update is useful in solving many issues facing administrators for ASA management, such as:

- Overcoming dynamic addressing and NAT challenges.
- Committing configuration changes in one action.
- Providing a reliable method for updating software.
- Leveraging well-understood methods for high availability (failover).
- Providing flexibility with an open interface.
- Simplifying security solutions for Service Provider environments.
The Auto Update specification provides the infrastructure necessary for remote management applications to download ASA configurations, software images, and to perform basic monitoring from a centralized location or multiple locations.

The Auto Update specification allows the Auto Update server to either push configuration information and send requests for information to the ASA, or to pull configuration information by having the ASA periodically poll the Auto Update server. The Auto Update server can also send a command to the ASA to send an immediate polling request at any time. Communication between the Auto Update server and the ASA requires a communications path and local CLI configuration on each ASA.

Auto Update Server Support in Failover Configurations

You can use the Auto Update Server to deploy software images and configuration files to ASAs in an Active/Standby failover configuration. To enable Auto Update on an Active/Standby failover configuration, enter the Auto Update Server configuration on the primary unit in the failover pair.

The following restrictions and behaviors apply to Auto Update Server support in failover configurations:

- Only single mode, Active/Standby configurations are supported.
- When loading a new platform software image, the failover pair stops passing traffic.
- When using LAN-based failover, new configurations must not change the failover link configuration. If they do, communication between the units will fail.
- Only the primary unit will perform the call home to the Auto Update Server. The primary unit must be in the active state to call home. If it is not, the ASA automatically fails over to the primary unit.
- Only the primary unit downloads the software image or configuration file. The software image or configuration is then copied to the secondary unit.
- The interface MAC address and hardware-serial ID is from the primary unit.
- The configuration file stored on the Auto Update Server or HTTP server is for the primary unit only.

Auto Update Process Overview

The following is an overview of the Auto Update process in failover configurations. This process assumes that failover is enabled and operational. The Auto Update process cannot occur if the units are synchronizing configurations, if the standby unit is in the failed state for any reason other than SSM card failure, or if the failover link is down.

1. Both units exchange the platform and ASDM software checksum and version information.
2. The primary unit contacts the Auto Update Server. If the primary unit is not in the active state, the ASA first fails over to the primary unit and then contacts the Auto Update Server.
3. The Auto Update Server replies with software checksum and URL information.
4. If the primary unit determines that the platform image file needs to be updated for either the active or standby unit, the following occurs:
   a. The primary unit retrieves the appropriate files from the HTTP server using the URL from the Auto Update Server.
   b. The primary unit copies the image to the standby unit and then updates the image on itself.
   c. If both units have new image, the secondary (standby) unit is reloaded first.
      - If hitless upgrade can be performed when secondary unit boots, then the secondary unit becomes the active unit and the primary unit reloads. The primary unit becomes the active unit when it has finished loading.
- If hitless upgrade cannot be performed when the standby unit boots, then both units reload at the same time.

d. If only the secondary (standby) unit has new image, then only the secondary unit reloads. The primary unit waits until the secondary unit finishes reloading.

e. If only the primary (active) unit has new image, the secondary unit becomes the active unit, and the primary unit reloads.

f. The update process starts again at Step 1.

5. If the ASA determines that the ASDM file needs to be updated for either the primary or secondary unit, the following occurs:

a. The primary unit retrieves the ASDM image file from the HTTP server using the URL provided by the Auto Update Server.

b. The primary unit copies the ASDM image to the standby unit, if needed.

c. The primary unit updates the ASDM image on itself.

d. The update process starts again at Step 1.

6. If the primary unit determines that the configuration needs to be updated, the following occurs:

a. The primary unit retrieves the configuration file from the using the specified URL.

b. The new configuration replaces the old configuration on both units simultaneously.

c. The update process begins again at Step 1.

7. If the checksums match for all image and configuration files, no updates are required. The process ends until the next poll time.

Monitoring the Auto Update Process

You can use the `debug auto-update client` or `debug fver cmd-exe` commands to display the actions performed during the Auto Update process. The following is sample output from the `debug auto-update client` command.

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
    Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum: 0x94bced0261cc992ae710faf8d244cf32
    Component: config, URL: http://192.168.0.21/config-rms.xml, checksum: 0x67358553572688a805a155af312f6898
    Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum: 0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
```
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 80
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419

The following syslog message is generated if the Auto Update process fails:

%ASA4-612002: Auto Update failed: file version: version reason: reason

The file is “image”, “asdm”, or “configuration”, depending on which update failed. The version is the version number of the update. And the reason is the reason that the update failed.

Guidelines and Limitations

- If HTTPS is chosen as the protocol to communicate with the Auto Update server, the ASA uses SSL, which requires the ASA to have a DES or 3DES license.
- Auto Update is supported in single context mode only.

Configuring Communication with an Auto Update Server

Detailed Steps

To configure the ASA as an Auto Update client, perform the following steps:

Step 1 To specify the URL of the Auto Update Server, enter the following command:
Cisco ASA Series General Operations CLI Configuration Guide

Chapter 36      Software and Configurations

Configuring Auto Update

ciscoasa(config)# auto-update server url [source interface] [verify-certificate | no-verification]

where url has the following syntax:
http[s]://[user:password@]server_ip[:port]/pathname

The source interface keyword and argument specify which interface to use when sending requests to the Auto Update Server. If you specify the same interface specified by the management-access command, the Auto Update requests travel over the same IPsec VPN tunnel used for management access.

For HTTPS, the verify-certificate keyword (the default) verifies the certificate returned by the Auto Update Server. To disable verification (not recommended), specify the no-verification keyword.

Step 2 (Optional) To identify the device ID to send when communicating with the Auto Update Server, enter the following command:
ciscoasa(config)# auto-update device-id {hardware-serial | hostname | ipaddress [if-name] | mac-address [if-name] | string text}

The identifier used is determined by specifying one of the following parameters:

- The hardware-serial argument specifies the ASA serial number.
- The hostname argument specifies the ASA hostname.
- The ipaddress keyword specifies the IP address of the specified interface. If the interface name is not specified, it uses the IP address of the interface used to communicate with the Auto Update Server.
- The mac-address keyword specifies the MAC address of the specified interface. If the interface name is not specified, it uses the MAC address of the interface used to communicate with the Auto Update Server.
- The string keyword specifies the specified text identifier, which cannot include white space or the characters ',', '', >, & and ?.

Step 3 (Optional) To specify how often to poll the Auto Update Server for configuration or image updates, enter the following command:
ciscoasa(config)# auto-update poll-period poll-period [retry-count [retry-period]]

The poll-period argument specifies how often (in minutes) to check for an update. The default is 720 minutes (12 hours).

The retry-count argument specifies how many times to try reconnecting to the server if the first attempt fails. The default is zero.

The retry-period argument specifies how long to wait (in minutes) between retries. The default is five minutes.

Step 4 (Optional) To schedule a specific time for the ASA to poll the Auto Update Server, enter the following command:
ciscoasa(config)# auto-update poll-at days-of-the-week time [randomize minutes] [retry_count [retry_period]]

The days-of-the-week argument is any single day or combination of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are daily (Monday through Sunday), weekdays (Monday through Friday), and weekends (Saturday and Sunday).

The time argument specifies the time in the format HH:MM at which to start the poll. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
The **randomize minutes** keyword and argument specify the period to randomize the poll time following the specified start time. The range is from 1 to 1439 minutes.

The **retry_count** argument specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is zero.

The **retry_period** argument specifies how long to wait between connection attempts. The default is five minutes. The range is from 1 to 35791 minutes.

### Step 5
(Optional) If the Auto Update Server has not been contacted for a certain period of time, entering the following command causes it to stop passing traffic:

```
ciscoasa(config)# auto-update timeout period
```

The **period** argument specifies the timeout period in minutes between 1 and 35791. The default is to never time out (zero minutes). To restore the default, enter the `no` form of this command.

Use the **auto-update timeout** command to be sure that the ASA has the most recent image and configuration. This condition is reported with system log message 201008.

In the following example, an ASA is configured to poll an Auto Update Server with the IP address 209.165.200.224, at port number 1742, from the outside interface, with certificate verification.

The ASA is also configured to use the hostname as the device ID and to poll an Auto Update Server every Friday and Saturday night at a random time between 10:00 p.m. and 11:00 p.m. On a failed polling attempt, the ASA will try to reconnect to the Auto Update Server ten times, and will wait three minutes between attempts at reconnecting, as shown in the following example:

```
ciscoasa(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside
verify-certificate
ciscoasa (config)# auto-update device-id hostname
hostname (config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
```

### Configuring Client Updates as an Auto Update Server

Entering the **client-update** command enables updates for ASAs configured as Auto Update clients and lets you specify the type of software component (ASDM or boot image), the type or family of ASA, revision numbers to which the update applies, and a URL or IP address from which to obtain the update.

To configure the ASA as an Auto Update Server, perform the following steps:

### Step 1
To enable client update, enter the following command:

```
ciscoasa(config)# client-update enable
```

### Step 2
Configure the following parameters for the **client-update** command that you want to apply to the ASAs:

```
client-update { component { asdm | image } | device-id dev_string | family family_name | type type } url url-string rev-nums rev-nums
```

The **component { asdm | image }** parameter specifies the software component, either ASDM or the boot image of the ASA.

The **device-id dev_string** parameter specifies a unique string that the Auto Update client uses to identify itself. The maximum length is 63 characters.

The **family family_name** parameter specifies the family name that the Auto Update client uses to identify itself. It can be asa, pix, or a text string with a maximum length of seven characters.
The `rev-nums` parameter specifies the software or firmware images for this client. Enter up to four, in any order, separated by commas.

The `type` parameter specifies the type of clients to notify of a client update. Because this command is also used to update Windows clients, the list of clients includes several Windows operating systems.

The `url url-string` parameter specifies the URL for the software/firmware image. This URL must point to a file appropriate for this client. For all Auto Update clients, you must use the protocol “http://” or “https://” as the prefix for the URL.

Configure the parameters for the client update that you want to apply to all ASAs of a particular type. That is, specify the type of ASA and the URL or IP address from which to get the updated image. In addition, you must specify a revision number. If the revision number of the remote ASA matches one of the specified revision numbers, there is no need to update the client, and the update is ignored.

To configure a client update for Cisco 5525-X ASAs, enter the following command:

```
ciscoasa(config)# client-update type asa5525 component asdm url http://192.168.1.114/aus/asdm601.bin rev-nums 8.0(1)
```

### Viewing Auto Update Status

To view the Auto Update status, enter the following command:

```
ciscoasa(config)# show auto-update
```

The following is sample output from the `show auto-update` command:

```
ciscoasa(config)# show auto-update
Server: https://********@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```
## Feature History for Software and Configurations

Table 36-1 lists each feature change and the platform release in which it was implemented.

### Table 36-1  Feature History for Software and Configurations

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Copy client</td>
<td>9.1(5)/9.2(1)</td>
<td>The ASA now supports the Secure Copy (SCP) client to transfer files to and from a SCP server. We introduced the following commands: <code>ssh pubkey-chain, server (ssh pubkey-chain), key-string, key-hash</code>, <code>ssh stricthostkeycheck</code>. We modified the following command: <code>copy scp</code>.</td>
</tr>
<tr>
<td>Auto Update server certificate verification enabled by default</td>
<td>9.2(1)</td>
<td>The Auto Update server certificate verification is now enabled by default; for new configurations, you must explicitly disable certificate verification. If you are upgrading from an earlier release, and you did not enable certificate verification, then certificate verification is not enabled, and you see the following warning: WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the <code>verify-certificate</code> option. The configuration will be migrated to explicitly configure no verification: <code>auto-update server no-verification</code> We modified the following command: `auto-update server {verify-certificate</td>
</tr>
<tr>
<td>System backup and restore using the CLI</td>
<td>9.3(2)</td>
<td>You can now back up and restore complete system configurations, including images and certificates, using the CLI. We introduced the following commands: <code>backup</code> and <code>restore</code>.</td>
</tr>
</tbody>
</table>
Response Automation for System Events

This chapter describes how to configure the Embedded Event Manager (EEM).

- About the EEM, page 37-1
- Guidelines for the EEM, page 37-2
- Configure the EEM, page 37-3
- Examples for the EEM, page 37-6
- Monitoring the EEM, page 37-7
- History for the EEM, page 37-8

About the EEM

The EEM service enables you to debug problems and provides general purpose logging for troubleshooting. There are two components: events to which the EEM responds or listens, and event manager applets that define actions as well as the events to which the EEM responds. You may configure multiple event manager applets to respond to different events and perform different actions.

Supported Events

The EEM supports the following events:

- Syslog—The ASA uses syslog message IDs to identify syslog messages that trigger an event manager applet. You may configure multiple syslog events, but the syslog message IDs may not overlap within a single event manager applet.

- Timers—You may use timers to trigger events. You may configure each timer only once for each event manager applet. Each event manager applet may have up to three timers. The three types of timers are the following:
  - Watchdog (periodic) timers trigger an event manager applet after the specified time period following the completion of the applet actions and restart automatically.
  - Countdown (one-shot) timers trigger an event manager applet once after the specified time period and do not restart unless they are removed, then re-added.
  - Absolute (once-a-day) timers cause an event to occur once a day at a specified time, and restart automatically. The time-of-day format is in hh:mm:ss.

You may configure only one timer event of each type for each event manager applet.
None—The none event is triggered when you run an event manager applet manually using the CLI or ASDM.

Crash—The crash event is triggered when the ASA crashes. Regardless of the value of the output command, the action commands are directed to the crashinfo file. The output is generated before the show tech command.

Actions on Event Manager Applets

When an event manager applet is triggered, the actions on the event manager applet are performed. Each action has a number that is used to specify the sequence of the actions. The sequence number must be unique within an event manager applet. You may configure multiple actions for an event manager applet. The commands are typical CLI commands, such as show blocks.

Output Destinations

You may send the output from the actions to a specified location using the output command. Only one output value may be enabled at any one time. The default value is output none. This value discards any output from the action commands. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled. You may send the output of the action CLI commands to one of three locations:

- None, which is the default and discards the output
- Console, which sends the output to the ASA console
- File, which sends the output to a file. The following four file options are available:
  - Create a unique file, which creates a new, uniquely named file each time that an event manager applet is invoked
  - Create/overwrite a file, which overwrites a specified file each time that an event manager applet is invoked.
  - Create/append to a file, which appends to a specified file each time that an event manager applet is invoked. If the file does not yet exist, it is created.
  - Create a set of files, which creates a set of uniquely named files that are rotated each time that an event manager applet is invoked.

Guidelines for the EEM

This section includes guidelines and limitations that you should check before configuring the EEM.

Context Mode Guidelines

Not supported in multiple context mode.

Additional Guidelines

- During a crash, the state of the ASA is generally unknown. Some commands may not be safe to run during this condition.
- The name of an event manager applet may not contain spaces.
- You cannot modify the None event and Crashinfo event parameters.
- Performance may be affected because syslog messages are sent to the EEM for processing.
Configure the EEM

Configuring the EEM consists of the following tasks:

---

**Step 1**  Create an event manager applet, then configure various events. See Create an Event Manager Applet and Configure Events, page 37-3.

**Step 2**  Configure an action on an event manager applet, then configure a destination for output from an action. See Configure an Action and Destinations for Output from an Action, page 37-5.

**Step 3**  Run an event manager applet. See Run an Event Manager Applet, page 37-6.

---

Create an Event Manager Applet and Configure Events

To create an event manager applet and configure events, perform the following steps:

**Procedure**

---

**Step 1**  Create an event manager applet and enter event manager applet configuration mode.

```
event manager applet name
```

Example:

```
ciscoasa(config)# event manager applet exampleapplet1
```

The `name` argument may be up to 32 alphanumeric characters long. Spaces are not allowed. To remove an event manager applet, enter the **no** form of this command.

**Step 2**  Describe an event manager applet.

```
description text
```

Example:

```
ciscoasa(config-applet)# description applet1example
```

The `text` argument may be up to 256 characters long. You may include spaces in description text if it is placed within quotes.

**Step 3**  To configure a specified event, enter one of the following commands. To remove the configured event, enter the **no** form of each of the commands.

- To configure a syslog event, identify a single syslog message or a range of syslog messages that trigger an event manager applet.

```
event syslog id nnnnnn[-nnnnnn] [occurs n] [period seconds]
```

Example:

```
ciscoasa(config-applet)# event syslog id 106201
```
Configure the EEM

The \texttt{nnnnnn} argument identifies the syslog message ID. The \texttt{occurs \textit{n}} keyword-argument pair indicates the number of times that the syslog message must occur for an event manager applet to be invoked. The default is 1 occurrence every 0 seconds. Valid values are from 1 - 4294967295. The \texttt{period \textit{seconds}} keyword-argument pair indicates the number of seconds in which the event must occur, and limits how frequently an event manager applet is invoked to at most once in the configured period. Valid values are from 0 - 604800. A value of 0 means that no period is defined.

- To configure an event to occur once per configured period and restart automatically.
  \texttt{event timer watchdog time \textit{seconds}}

  Example:
  \begin{verbatim}
  ciscoasa(config-applet)# event timer watchdog time 30
  \end{verbatim}

  The number of seconds may range from 1 - 604800.

- To configure an event to occur once and not restart unless it is removed, then re-added.
  \texttt{event timer countdown time \textit{seconds}}

  Example:
  \begin{verbatim}
  ciscoasa(config-applet)# event timer countdown time 60
  \end{verbatim}

  The number of seconds may range from 1 - 604800. Use the \texttt{no} form of this command remove a countdown timer event.

  \textbf{Note}\hspace{1cm} This timer reruns when you reboot if it is the startup configuration.

- To configure an event to occur once a day at a specified time and restart automatically.
  \texttt{event timer absolute time \textit{hh:mm:ss}}

  Example:
  \begin{verbatim}
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  \end{verbatim}

  The time-of-day format is in hh:mm:ss. The time range is from 00:00:00 (midnight) to 23:59:59.

- Trigger a crash event when the ASA crashes.
  \texttt{event crashinfo}

  Example:
  \begin{verbatim}
  ciscoasa(config-applet)# event crashinfo
  \end{verbatim}

  Regardless of the value of the \texttt{output} command, the \texttt{action} commands are directed to the crashinfo file. The output is generated before the \texttt{show tech} command.
Configure an Action and Destinations for Output from an Action

To configure an action and specific destinations for sending output from an action, perform the following steps:

**Procedure**

**Step 1** Configure an action on an event manager applet.

```
action n cli command "command"
```

Example:
```
ciscoasa(config-applet)# action 1 cli command "show version"
```

The `n` option is an action ID. Valid IDs range from 0 - 4294967295. The value of the `command` option must be in quotes; otherwise, an error occurs if the command consists of more than one word. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled. Use the `noconfirm` option if the command has it available.

**Step 2** Choose one of the available output destination options. Use the `no` form of each command to remove an output destination,

- The **None** option discards any output from the `action` commands, which is the default setting:

```
output none
```

Example:
```
ciscoasa(config-applet)# output none
```

- The **Console** option sends the output of the `action` commands to the console.

```
output console
```

Example:
```
ciscoasa(config-applet)# output console
```

**Note** Running this command affects performance.

- The **New File** option sends the output of the `action` commands to a new file for each event manager applet that is invoked.

```
output file new
```

Example:
```
ciscoasa(config-applet)# output file new
```

The filename has the format of `eem-applet-timestamp.log`, in which `applet` is the name of the event manager applet and `timestamp` is a dated time stamp in the format of `YYYYMMDD-hhmmss`.

- The **New Set of Rotated Files** option creates a set of files that are rotated. When a new file is to be written, the oldest file is deleted, and all subsequent files are renumbered before the first file is written.

```
output file rotate n
```
Example:

ciscoasa(config-applet)# output file rotate 50

The newest file is indicated by 0, and the oldest file is indicated by the highest number \((n-1)\). The \(n\) option is the rotate value. Valid values range from 2 - 100. The filename format is eem-applet-x.log, in which \(applet\) is the name of the applet, and \(x\) is the file number.

- The **Single Overwritten File** option writes the **action** command output to a single file, which is overwritten every time.

  `output file overwrite filename`

Example:

ciscoasa(config-applet)# output file overwrite examplefile1

The `filename` argument is a local (to the ASA) filename. This command may also use FTP, TFTP, and SMB targeted files.

- The **Single Appended File** option writes the **action** command output to a single file, but that file is appended to every time.

  `output file append filename`

Example:

ciscoasa(config-applet)# output file append examplefile1

The `filename` argument is a local (to the ASA) filename.

---

**Run an Event Manager Applet**

To run an event manager applet, perform the following steps:

**Procedure**

**Step 1** Run an event manager applet.

`event manager run applet`

Example:

ciscoasa# event manager run exampleapplet1

If you run an event manager applet that has not been configured with the **event none** command, an error occurs. The `applet` argument is the name of the event manager applet.

---

**Examples for the EEM**

The following example shows an event manager applet that records block leak information every hour and writes the output to a rotating set of log files, keeping a day’s worth of logs:

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description “Log block usage”
```
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24

ciscoasa(config-applet)# action 1 cli command “show blocks old”

The following example shows an event manager applet that reboots the ASA every day at 1 am, saving the configuration as needed:

ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description “Reboot every night”
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none

ciscoasa(config-applet)# action 1 cli command “reload save-config noconfirm”

The following example shows event manager applets that disable the given interface between midnight and 3 am.

ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description “Disable the interface at midnight”
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none

ciscoasa(config-applet)# action 1 cli command “interface GigabitEthernet 0/0”
ciscoasa(config-applet)# action 2 cli command “shutdown”
ciscoasa(config-applet)# action 3 cli command “write memory”

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description “Enable the interface at 3am”
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none

ciscoasa(config-applet)# action 1 cli command “interface GigabitEthernet 0/0”
ciscoasa(config-applet)# action 2 cli command “no shutdown”
ciscoasa(config-applet)# action 3 cli command “write memory”

Monitoring the EEM

See the following commands to monitor the EEM.

- **clear configure event manager**
  This command removes the event manager running configuration.

- **clear configure event manager applet appletname**
  This command removes the named event manager applet from the configuration.

- **show counters protocol eem**
  This command shows the counters for the event manager.

- **show event manager**
  This command shows information about the configured event manager applets, including hit counts and when the event manager applets were last invoked.

- **show running-config event manager**
  This command shows the running configuration of the event manager.
History for the EEM

Table 37-1  History for the EEM

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Event Manager (EEM)</td>
<td>9.2(1)</td>
<td>The EEM service enables you to debug problems and provides general purpose logging for troubleshooting. There are two components: events to which the EEM responds or listens, and event manager applets that define actions as well as the events to which the EEM responds. You may configure multiple event manager applets to respond to different events and perform different actions. We introduced or modified the following commands: <code>event manager applet</code>, <code>description</code>, <code>event syslog id</code>, <code>event none</code>, <code>event timer</code> `{ watchdog time seconds</td>
</tr>
</tbody>
</table>
Troubleshooting

This chapter describes how to troubleshoot the Cisco ASA.

- View Debugging Messages, page 38-1
- Capture Packets, page 38-1
- View the Crash Dump, page 38-5
- View the Coredump, page 38-5
- vCPU Usage in the ASAv, page 38-5

View Debugging Messages

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use `debug` commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use `debug` commands during periods of less network traffic and fewer users. Debugging during these periods decreases the likelihood that increased `debug` command processing overhead will affect system use. To enable debugging messages, see the `debug` commands in the command reference.

Capture Packets

Capturing packets may be useful when troubleshooting connectivity problems or monitoring suspicious activity. We recommend that you contact Cisco TAC if you want to use the packet capture service.

To capture packets, perform the following steps:

**Procedure**

**Step 1**

Enable packet capture capabilities for packet sniffing and network fault isolation.

```
[cluster exec] capture capture_name [type {asp-drop all [drop-code] | tls-proxy | raw-data | lACP | isakmp [ikev1 | ikev2] | inline-tag [tag] | webvpn user webvpn-user}] [access-list access_list_name] [interface asa_dataplane] [buffer buf_size] [ethernet-type type] [interface interface_name] [reinject-hide] [packet-length bytes] [circular-buffer] [trace trace_count] [real-time] [trace] [match prot {host source-ip | source-ip mask | any} host destination-ip | destination-ip mask | any} [operator port]
```

Example:
Capture Packets

For the complete syntax description, see the command reference or the CLI help (help capture). Not all options can be specified in one command. See the CLI help for allowed combinations.

Use the same capture_name on multiple capture statements to capture multiple types of traffic.

The type asp-drop keyword captures packets dropped by the accelerated security path. In a cluster, dropped forwarded data packets from one unit to another are also captured. In multiple context mode, when this option is issued in system context, all dropped data packets are captured; when this option is issued in a user context, only dropped data packets that enter from interfaces belonging to the user context are captured.

The inline-tag tag keyword-argument pair specifies a tag for a particular SGT value or leaves it unspecified to capture a tagged packet with any SGT value.

The buffer keyword defines the buffer size used to store the packet. When the byte buffer is full, packet capture stops. When used in a cluster, this is the per-unit size, not the sum of all units. The circular-buffer keyword overwrites the buffer, starting from the beginning, when the buffer is full.

The interface keyword sets the name of the interface on which to use packet capture. You must configure an interface for any packets to be captured.

To capture packets on the dataplane, use the asa_dataplane keyword. To filter packets captured on the ASA CX backplane, use the asa_dataplane option and follow these guidelines. In single mode, the backplane control packets bypass the access list and are captured. In multiple context mode, only control packets are captured in the system context. Data packets are captured in the user context. The access-list and match options are only available in the user context.

To capture the traffic on the cluster control link, use the cluster keyword. If you configure type lacp, specify the physical interface ID instead of the nameif name.

The match keyword captures matching the protocol and source and destination IP addresses and optional ports. You can use this keyword up to three times in one command. The operator can be one of the following:

- lt—less than
- gt—greater than
- eq—equal to

The type raw-data keywords capture inbound and outbound packets. This setting is the default.

The real-time keyword displays the captured packets continuously in real-time. To terminate real-time packet capture, enter Ctrl + c. To permanently remove the capture, use the no form of this command. This option applies only to raw-data and asp-drop captures. This option is not supported when you use the cluster exec capture command.

The reinject-hide keyword specifies that no reinjected packets will be captured and applies only in a clustering environment.

Note: If ACL optimization is configured, you cannot use the access-list command in capture. You can only use the access-group command. An error appears if you try to use the access-list command in this case.
Capture Packets in a Clustering Environment

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.

The “cluster” interface name is the default name for the cluster control link and is not configurable. You specify “cluster” as the interface name to capture the traffic on the cluster control link interface. There are two types of packets on the cluster control link: control plane packets and data plane packets, which both include forwarded data traffic and cluster LU messages. The TTL field in the IP address header is encoded to differentiate between these two types of packets. When forwarded data packets are captured, their clustering trailers are included in the capture file for debugging purposes.

In multiple context mode, although the cluster interface belongs to the system context, you can see the interface, so you can configure captures on the cluster link in user contexts. In the system context, both control plane and data plane packets are available. The data plane captures LU packets and forwarded data packets that belong only to the system context. In user contexts, control plane packets are not visible. Only forwarded data packets that belong to a specified user context and LU packets are captured. For security purposes, each context can only see the packets that belong to it.

Guidelines for Capturing Packets

- If the ASA receives packets with an incorrectly formatted TCP header and drops them because of the `invalid-tcp-hdr-length` ASP drop reason, the `show capture` command output on the interface where those packets are received does not show those packets.
- You can only capture IP traffic; you cannot capture non-IP packets such as ARPs.
- For cluster control link capture in multiple context mode, only the packet that is associated with the context sent in the cluster control link is captured.
- For inline SGT tagged packets, captured packets contain an additional CMD header that your PCAP viewer might not understand.
- In multiple context mode, the `copy capture` command is available only in the system space. The syntax is as follows:

  `copy pcap capture:Context-name/in-cap tftp:`

  Where `in-cap` is the capture configured in the context `context-name`
- The `cluster exec capture realtime` command is not supported. The following error message appears:

  Error: Real-time capture can not be run in cluster exec mode.
- For a shared VLAN, the following guidelines apply:
  - You can only configure one capture for the VLAN; if you configure a capture in multiple contexts on the shared VLAN, then only the last capture that was configured is used.
  - If you remove the last-configured (active) capture, no captures become active, even if you have previously configured a capture in another context; you must remove the capture and add it again to make it active.
  - All traffic that enters the interface to which the capture is attached is captured, including traffic to other contexts on the shared VLAN.
Therefore, if you enable a capture in Context A for a VLAN that is also used by Context B, both Context A and Context B ingress traffic are captured.

- For egress traffic, only the traffic of the context with the active capture is captured. The only exception is when you do not enable the ICMP inspection (therefore the ICMP traffic does not have a session in the accelerated path). In this case, both ingress and egress ICMP traffic for all contexts on the shared VLAN is captured.

- Configuring a capture typically involves configuring an ACL that matches the traffic that needs to be captured. After an ACL that matches the traffic pattern is configured, then you need to define a capture and associate this ACL to the capture, along with the interface on which the capture needs to be configured.

- After you have performed a cluster-wide capture, to copy the same cluster-wide capture file to a TFTP server, enter the following command on the master unit:

  ```
ciscoasa (cfg-cluster)# cluster exec copy /pcap capture: cap_name tftp://location/path/filename.pcap
  ```

- Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as filename_A.pcap, filename_B.pcap, and so on. In this example, A and B are cluster unit names. A different destination name is generated if you add the unit name at the end of the filename.

- To enable cluster-wide capture on a specified interface, you can add the `cluster exec` keywords in front of each of the commands shown in the examples. These `capture` commands can only be replicated from the master unit to the slave units. However, you can still configure a capture on the specified interface for the local unit using any of these `capture` commands.

### Examples

The following example shows how to create a cluster-wide LACP capture:

```
ciscoasa (config)# cluster exec capture lacp type lacp interface gigabitEthernet0/0
```

The following example shows how to create a capture for control path packets in the clustering link:

```
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
```

The following example shows how to create a capture for data path packets in the clustering link:

```
ciscoasa (config)# access-list ccl extended permit udp any eq 4193
```

```
ciscoasa (config)# access-list ccl extended permit udp any eq 4193 any
```

```
ciscoasa (config)# capture dp interface cluster access-list ccl
```

The following example shows how to capture data path traffic through the cluster:

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
```

```
ciscoasa (config)# capture abc interface inside match udp host 1.1.1.1 any
```

```
ciscoasa (config)# capture abc interface inside access-list xxx
```

The following example shows how to capture logical update messages for flows that match the real source to the real destination, and capture packets forwarded over CCL that match the real source to the real destination:

```
ciscoasa (config)# access-list dp permit ip real_src real_dst
```

The following example shows how to capture a certain type of data plane message, such as icmp echo request/response, that is forwarded from one ASA to another ASA using the `match` keyword or the ACL for the message type:

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```
The following example shows how to create a capture by using ACL 103 on a cluster control link:

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster access-list 103
```

In the previous example, if A and B are IP addresses for the CCL interface, only the packets that are sent between these two units are captured.

If A and B are IP addresses for through-device traffic, then the following is true:

- Forwarded packets are captured as usual, provided the source and destination IP addresses are matched with the ACL.
- The data path logic update message is captured provided it is for the flow between A and B or for an ACL (for example, access-list 103). The capture matches the five-tuple of the embedded flow.

Although the source and destination addresses in the UDP packet are CCL addresses, if this packet is to update a flow that is associated with addresses A and B, then it is also captured. That is, as long as addresses A and B that are embedded in the packet are matched, it is also captured.

**View the Crash Dump**

If the ASA or ASAv crashes, you can view the crash dump information. We recommend that you contact Cisco TAC if you want to interpret the crash dump. See the `show crashdump` command in the command reference.

**View the Coredump**

A coredump is a snapshot of the running program when the program has terminated abnormally or crashed. Coredumps are used to diagnose or debug errors and save a crash for future off-site analysis. Cisco TAC may request that you enable the coredump feature to troubleshoot application or system crashes on the ASA or ASAv. See the `coredump` command in the command reference.

**vCPU Usage in the ASAv**

The ASAv vCPU usage shows the amount of vCPUs used for the data path, control point, and external processes.

The vSphere reported vCPU usage includes the ASAv usage as described plus:

- ASAv idle time
- %SYS overhead used for the ASAv VM
- Overhead of moving packets between vSwitches, vNICs, and pNICs. This overhead can be quite significant.

**CPU Usage Example**

The following is an example in which the reported vCPU usage is substantially different:

- ASAv reports: 40%
vCPU Usage in the ASAv

- DP: 35%
- External Processes: 5%
- vSphere reports: 95%
- ASA (as ASAv reports): 40%
- ASA idle polling: 10%
- Overhead: 45%

The overhead is used to perform hypervisor functions and to move packets between NICs and vNICs using the vSwitch.

Usage can exceed 100% because the ESXi server can use additional compute resources for overhead on behalf of the ASAv.

VMware CPU Usage Reporting

In vSphere, click the VM Performance tab, then click Advanced to display the Chart Options drop-down list, which shows vCPU usage for each state (%USER, %IDLE, %SYS, and so on) of the VM. This information is useful for understanding VMware’s perspective on where CPU resources are being used.

On the ESXi server shell (you access the shell by using SSH to connect to the host), esxtop is available. Esxtop has a similar look and feel to the Linux top command and provides VM state information for vSphere performance, including the following:
- Details on vCPU, memory, and network usage
- vCPU usage for each state of each VM.
- Memory (type M while running) and network (type N while running), as well as statistics and the number of RX drops

ASAv and vCenter Graphs

There are differences in the CPU % numbers between the ASAv and vCenter:
- The vCenter graph numbers are always higher than the ASAv numbers.
- vCenter calls it %CPU usage; the ASAv calls it %CPU utilization.

The terms “%CPU utilization” and “%CPU usage” mean different things:
- CPU utilization provides statistics for physical CPUs.
- CPU usage provides statistics for logical CPUs, which is based on CPU hyperthreading. But because only one vCPU is used, hyperthreading is not turned on.

vCenter calculates the CPU % usage as follows:

\[ \frac{\text{Amount of actively used virtual CPUs}}{\text{number of virtual CPUs} \times \text{core frequency}} \]

This calculation is the host view of the CPU usage, not the guest operating system view, and is the average CPU utilization over all available virtual CPUs in the virtual machine.

For example, if a virtual machine with one virtual CPU is running on a host that has four physical CPUs and the CPU usage is 100%, the virtual machine is using one physical CPU completely. The virtual CPU usage calculation is as follows:

Usage in MHz / number of virtual CPUs x core frequency
When you compare the usage in MHz, both the vCenter and ASA numbers match. According to the vCenter graph, MHz % CPU usage is calculated as:

\[
\frac{60}{(2499 \times 1 \text{ vCPU})} = 2.4
\]
PART 9

Logging, SNMP, and Smart Call Home
This chapter describes how to log system messages and use them for troubleshooting.

- About Logging, page 39-1
- Guidelines for Logging, page 39-5
- Configure Logging, page 39-6
- Monitoring the Logs, page 39-19
- Examples for Logging, page 39-20
- History for Logging, page 39-21

About Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

The Cisco ASA system logs provide you with information for monitoring and troubleshooting the ASA. With the logging feature, you can do the following:

- Specify which syslog messages should be logged.
- Disable or change the severity level of a syslog message.
- Specify one or more locations where syslog messages should be sent, including an internal buffer, one or more syslog servers, ASDM, an SNMP management station, specified e-mail addresses, or to Telnet and SSH sessions.
- Configure and manage syslog messages in groups, such as by severity level or class of message.
- Specify whether or not a rate-limit is applied to syslog generation.
- Specify what happens to the contents of the internal log buffer when it becomes full: overwrite the buffer, send the buffer contents to an FTP server, or save the contents to internal flash memory.
- Filter syslog messages by locations, severity level, class, or a custom message list.
Logging in Multiple Context Mode

Each security context includes its own logging configuration and generates its own messages. If you log in to the system or admin context, and then change to another context, messages you view in your session are only those messages that are related to the current context.

Syslog messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure logging or view any logging information in the system execution space.

You can configure the ASA and ASASM to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of system, and messages that originate in the admin context use the name of the admin context as the device ID.

Syslog Message Analysis

The following are some examples of the type of information you can obtain from a review of various syslog messages:

- Connections that are allowed by ASA and ASASM security policies. These messages help you spot holes that remain open in your security policies.
- Connections that are denied by ASA and ASASM security policies. These messages show what types of activity are being directed toward your secured inside network.
- Using the ACE deny rate logging feature shows attacks that are occurring on your ASA or ASA Services Module.
- IDS activity messages can show attacks that have occurred.
- User authentication and command usage provide an audit trail of security policy changes.
- Bandwidth usage messages show each connection that was built and torn down as well as the duration and traffic volume used.
- Protocol usage messages show the protocols and port numbers used for each connection.
- Address translation audit trail messages record NAT or PAT connections being built or torn down, which are useful if you receive a report of malicious activity coming from inside your network to the outside world.

Syslog Message Format

Syslog messages begin with a percent sign (%) and are structured as follows:

%ASA  Level Message_number: Message_text

Field descriptions are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA</td>
<td>The syslog message facility code for messages that are generated by the ASA and ASASM. This value is always ASA.</td>
</tr>
<tr>
<td>Level</td>
<td>1 through 7. The level reflects the severity of the condition described by the syslog message—the lower the number, the more severe the condition.</td>
</tr>
</tbody>
</table>
About Logging

Severity Levels

Table 39-1 lists the syslog message severity levels. You can assign custom colors to each of the severity levels to make it easier to distinguish them in the ASDM log viewers. To configure syslog message color settings, either choose the Tools > Preferences > Syslog tab or, in the log viewer itself, click Color Settings on the toolbar.

<table>
<thead>
<tr>
<th>Level Number</th>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>emergencies</td>
<td>System is unusable.</td>
</tr>
<tr>
<td>1</td>
<td>alert</td>
<td>Immediate action is needed.</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
<td>Critical conditions.</td>
</tr>
<tr>
<td>3</td>
<td>error</td>
<td>Error conditions.</td>
</tr>
<tr>
<td>4</td>
<td>warning</td>
<td>Warning conditions.</td>
</tr>
<tr>
<td>5</td>
<td>notification</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td>6</td>
<td>informational</td>
<td>Informational messages only.</td>
</tr>
<tr>
<td>7</td>
<td>debugging</td>
<td>Debugging messages only.</td>
</tr>
</tbody>
</table>

Note: The ASA and ASASM do not generate syslog messages with a severity level of zero (emergencies). This level is provided in the logging command for compatibility with the UNIX syslog feature, but is not used by the ASA.

Message Classes and Range of Syslog IDs

For a list of syslog message classes and the ranges of syslog message IDs that are associated with each class, see the syslog messages guide.

Syslog Message Filtering

You can filter generated syslog messages so that only certain syslog messages are sent to a particular output destination. For example, you could configure the ASA and ASASM to send all syslog messages to one output destination and to send a subset of those syslog messages to a different output destination.

Specifically, you can configure the ASA and ASASM so that syslog messages are directed to an output destination according to the following criteria:

- Syslog message ID number
- Syslog message severity level
- Syslog message class (equivalent to a functional area of the ASA and ASASM)
You customize these criteria by creating a message list that you can specify when you set the output destination. Alternatively, you can configure the ASA or ASASM to send a particular message class to each type of output destination independently of the message list.

You can use syslog message classes in two ways:

- Specify an output location for an entire category of syslog messages using the `logging class` command.
- Create a message list that specifies the message class using the `logging list` command.

The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the ASA and ASASM. For example, the `vpnc` class denotes the VPN client.

All syslog messages in a particular class share the same initial three digits in their syslog message ID numbers. For example, all syslog message IDs that begin with the digits 611 are associated with the `vpnc` (VPN client) class. Syslog messages associated with the VPN client feature range from 611101 to 611323.

In addition, most of the ISAKMP syslog messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a syslog message when available. If the object is not known at the time that the syslog message is generated, the specific `heading = value` combination does not appear.

The objects are prefixed as follows:

```
Group = groupname, Username = user, IP = IP_address
```

Where the group is the tunnel-group, the username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or Layer 2 peer.

### Custom Message Lists

Creating a custom message list is a flexible way to exercise control over which syslog messages are sent to which output destination. In a custom syslog message list, you specify groups of syslog messages using any or all of the following criteria: severity level, message IDs, ranges of syslog message IDs, or message class.

For example, you can use message lists to do the following:

- Select syslog messages with the severity levels of 1 and 2 and send them to one or more e-mail addresses.
- Select all syslog messages associated with a message class (such as `ha`) and save them to the internal buffer.

A message list can include multiple criteria for selecting messages. However, you must add each message selection criterion with a new command entry. It is possible to create a message list that includes overlapping message selection criteria. If two criteria in a message list select the same message, the message is logged only once.

### Clustering

Syslog messages are an invaluable tool for accounting, monitoring, and troubleshooting in a clustering environment. Each ASA unit in the cluster (up to eight units are allowed) generates syslog messages independently; certain `logging` commands then enable you to control header fields, which include a time.
Guidelines for Logging

This section includes the guidelines and limitations that you should check before configuring logging.

IPv6 Guidelines
Does not support IPv6.

Additional Guidelines

- The syslog server must run a server program called syslogd. Windows (except for Windows 95 and Windows 98) provides a syslog server as part of its operating system. For Windows 95 and Windows 98, you must obtain a syslogd server from another vendor.

- To view logs generated by the ASA or ASASM, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the ASA and ASASM generate messages but does not save them to a location from which you can view them. You must specify each different logging output destination separately. For example, to designate more than one syslog server as an output destination, enter a new command for each syslog server.

- Sending syslogs over TCP is not supported on a standby ASA.

- The ASA supports the configuration of 16 syslog servers with the logging host command in single context mode. In multiple context mode, the limitation is 4 servers per context.

- The syslog server should be reachable through the ASA and ASASM. You should configure the ASASM to deny ICMP unreachable messages on the interface through which the syslog server is reachable and to send syslogs to the same server. Make sure that you have enabled logging for all severity levels. To prevent the syslog server from crashing, suppress the generation of syslogs 313001, 313004, and 313005.

- When you use a custom message list to match only access list hits, the access list logs are not generated for access lists that have had their logging severity level increased to debugging (level 7). The default logging severity level is set to 6 for the logging list command. This default behavior is by design. When you explicitly change the logging severity level of the access list configuration to debugging, you must also change the logging configuration itself.

The following is sample output from the show running-config logging command that does not include access list hits, because their logging severity level has been changed to debugging:

ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test

The following is sample output from the show running-config logging command that does include access list hits:

ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered debugging
Configure Logging

This section describes how to configure logging.

**Step 1**

**Step 2**

**Note**
The minimum configuration depends on what you want to do and what your requirements are for handling syslog messages in the ASA and ASASM.

Enable Logging

To enable logging, perform the following steps:

**Procedure**

**Step 1**
Enable logging.

```
logging enable
```

Example:
```
ciscoasa(config)# logging enable
```

Configure an Output Destination

To optimize syslog message usage for troubleshooting and performance monitoring, we recommend that you specify one or more locations where syslog messages should be sent, including an internal log buffer, one or more external syslog servers, ASDM, an SNMP management station, the console port, specified e-mail addresses, or Telnet and SSH sessions.
Send Syslog Messages to an External Syslog Server

You can archive messages according to the available disk space on the external syslog server, and manipulate logging data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

To send syslog messages to an external syslog server, perform the following steps:

**Procedure**

**Step 1** Configure the ASA and ASASM to send messages to a syslog server.

```
logging host interface_name syslog_ip [tcp[/port] | udp[/port] [format emblem]]
```

Example:

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem
```

The `format emblem` keyword enables EMBLEM format logging for the syslog server with UDP only. The `interface_name` argument specifies the interface through which you access the syslog server. The `syslog_ip` argument specifies the IP address of the syslog server. The `tcp[/port]` or `udp[/port]` keyword and argument pair specify that the ASA and ASASM should use TCP or UDP to send syslog messages to the syslog server.

You can configure the ASA to send data to a syslog server using either UDP or TCP, but not both. The default protocol is UDP if you do not specify a protocol.

If you specify TCP, the ASA and ASASM discover when the syslog server fails and as a security protection, new connections through the ASA and ASAM Services Module are blocked. To allow new connections regardless of connectivity to a TCP syslog server, see Step 3. If you specify UDP, the ASA and ASASM continue to allow new connections whether or not the syslog server is operational. Valid port values for either protocol are 1025 through 65535. The default UDP port is 514. The default TCP port is 1470.

**Step 2** Specify which syslog messages should be sent to the syslog server.

```
logging trap {severity_level | message_list}
```

Example:

```
ciscoasa(config)# logging trap errors
```

You can specify the severity level number (1 through 7) or name. For example, if you set the severity level to 3, then the ASA and ASASM send syslog messages for severity levels 3, 2, and 1. You can specify a custom message list that identifies the syslog messages to send to the syslog server.

**Step 3** (Optional) Disable the feature to block new connections when a TCP-connected syslog server is down.

```
logging permit-hostdown
```

Example:

```
ciscoasa(config)# logging permit-hostdown
```

If the ASA or ASASM is configured to send syslog messages to a TCP-based syslog server, and if either the syslog server is down or the log queue is full, then new connections are blocked. New connections are allowed again after the syslog server is back up and the log queue is no longer full.

**Step 4** (Optional) Set the logging facility to a value other than 20, which is what most UNIX systems expect.

```
logging facility number
```

Example:

```
ciscoasa(config)# logging facility
```
Send Syslog Messages to the Internal Log Buffer

You need to specify which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location. New messages are appended to the end of the list. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated, unless you configure the ASA and ASASM to save the full buffer to another location.

To send syslog messages to the internal log buffer, perform the following steps:

Procedure

Step 1 Specify which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location.

Example:

ciscoasa(config)# logging buffered critical

ciscoasa(config)# logging buffered level 2

ciscoasa(config)# logging buffered notif-list

New messages are appended to the end of the list. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated, unless you configure the ASA and ASASM to save the full buffer to another location. To empty the internal log buffer, enter the clear logging buffer command.

Step 2 Change the size of the internal log buffer. The default buffer size is 4 KB.

Example:

ciscoasa(config)# logging buffer-size 16384

Step 3 Choose one of the following options:

- Save new messages to the internal log buffer and save the full log buffer content to the internal flash memory.

  Example:

  ciscoasa(config)# logging flash-bufferwrap

- Save new messages to the internal log buffer and save the full log buffer content to an FTP server.

  Example:

  ciscoasa(config)# logging ftp-bufferwrap
Example:
ciscoasa(config)# logging flash-bufferwrap

When saving the buffer content to another location, the ASA and ASASM create log files with names that use the following time-stamp format:

LOG-YYYY-MM-DD-HHMMSS.TXT

where YYYY is the year, MM is the month, DD is the day of the month, and HHMMSS is the time in hours, minutes, and seconds.

- Identify the FTP server on which you want to store log buffer content.

logging ftp-server server path username password

Example:
ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs

The server argument specifies the IP address of the external FTP server. The path argument specifies the directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. The username argument specifies a username that is valid for logging into the FTP server. The password argument indicates the password for the username specified.

- Save the current log buffer content to the internal flash memory.

logging savelog [savefile]

Example:
ciscoasa(config)# logging savelog latestlogfile.txt

---

**Send Syslog Messages to an E-mail Address**

To send syslog messages to an e-mail address, perform the following steps:

**Procedure**

**Step 1** Specify which syslog messages should be sent to an e-mail address.

logging mail (severity_level | message_list)

Example:
ciscoasa(config)# logging mail high-priority

When sent by e-mail, a syslog message appears in the subject line of the e-mail message. For this reason, we recommend configuring this option to notify administrators of syslog messages with high severity levels, such as critical, alert, and emergency.

**Step 2** Specify the source e-mail address to be used when sending syslog messages to an e-mail address.

logging from-address email_address

Example:
ciscoasa(config)# logging from-address xxx-001@example.com

**Step 3** Specify the recipient e-mail address to be used when sending syslog messages to an e-mail address.
logging recipient-address e-mail_address [severity_level]

Example:
ciscoasa(config)# logging recipient-address admin@example.com

Step 4 Specify the SMTP server to be used when sending syslog messages to an e-mail address.
smtp-server ip_address

Example:
ciscoasa(config)# smtp-server 10.1.1.1

Send Syslog Messages to ASDM

To send syslog messages to ASDM, perform the following steps:

Procedure

Step 1 Specify which syslog messages should be sent to ASDM.
logging asdm {severity_level | message_list}

Example:
ciscoasa(config)# logging asdm 2

The ASA or ASASM sets aside a buffer area for syslog messages waiting to be sent to ASDM and saves messages in the buffer as they occur. The ASDM log buffer is a different buffer than the internal log buffer. When the ASDM log buffer is full, the ASA or ASASM deletes the oldest syslog message to make room in the buffer for new ones. Deletion of the oldest syslog message to make room for new ones is the default setting in ASDM. To control the number of syslog messages retained in the ASDM log buffer, you can change the size of the buffer.

Step 2 Specify the number of syslog messages to be retained in the ASDM log buffer.
logging asdm-buffer-size num_of_msgs

Example:
ciscoasa(config)# logging asdm-buffer-size 200

Enter the clear logging asdm command to empty the current content of the ASDM log buffer.
Send Syslog Messages to the Console Port

To send syslog messages to the console port, perform the following steps:

**Procedure**

**Step 1** Specify which syslog messages should be sent to the console port.

```
logging console {severity_level | message_list}
```

Example:
```
ciscoasa(config)# logging console errors
```

Send Syslog Messages to an SNMP Server

To enable logging to an SNMP server, perform the following steps:

**Step 1** Enable SNMP logging and specify which messages are to be sent to SNMP servers.

```
logging history [logging_list | level]
```

Example:
```
ciscoasa(config)# logging history errors
```

Enter the no logging history command to disable SNMP logging.

Send Syslog Messages to a Telnet or SSH Session

To send syslog messages to a Telnet or SSH session, perform the following steps:

**Procedure**

**Step 1** Specify which syslog messages should be sent to a Telnet or SSH session.

```
logging monitor {severity_level | message_list}
```

Example:
```
ciscoasa(config)# logging monitor 6
```

**Step 2** Enable logging to the current session only.

```
terminal monitor
```

Example:
```
ciscoasa(config)# terminal monitor
```
Configuring Logging

If you log out and then log in again, you need to reenter this command. Enter the terminal no monitor command to disable logging to the current session.

Create a Custom Event List

You use the following three criteria to define an event list:

- Event Class
- Severity
- Message ID

To create a custom event list to send to a specific logging destination (for example, an SNMP server), perform the following steps:

**Procedure**

**Step 1** Specify criteria for selecting messages to be saved in the internal log buffer. For example, if you set the severity level to 3, then the ASA sends syslog messages for severity levels 3, 2, and 1.

```
logging list name {level level [class message_class] | message start_id[-end_id]}
```

Example:
```
ciscoasa(config)# logging list notif-list level 3
```

The name argument specifies the name of the list. The level level keyword and argument pair specify the severity level. The class message_class keyword and argument pair specify a particular message class. The message start_id[-end_id] keyword and argument pair specify an individual syslog message number or a range of numbers.

**Note** Do not use the names of severity levels as the name of a syslog message list. Prohibited names include emergencies, alert, critical, error, warning, notification, informational, and debugging. Similarly, do not use the first three characters of these words at the beginning of an event list name. For example, do not use an event list name that starts with the characters “err.”

**Step 2** (Optional) Add more criteria for message selection to the list.

```
logging list name {level level [class message_class] | message start_id[-end_id]}
```

Example:
```
ciscoasa(config)# logging list notif-list message 104024-105999
```
```
ciscoasa(config)# logging list notif-list level critical
```
```
ciscoasa(config)# logging list notif-list level warning class ha
```

Enter the same command as in the previous step, specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion that you want to add to the list. For example, you can specify criteria for syslog messages to be included in the list as the following:

- Syslog message IDs that fall into the range of 104024 to 105999.
- All syslog messages with the critical severity level or higher (emergency, alert, or critical).
Configure Logging

- All ha class syslog messages with the warning severity level or higher (emergency, alert, critical, error, or warning).

**Note** A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.

### Generate Syslog Messages in EMBLEM Format to a Syslog Server

To generate syslog messages in EMBLEM format to a syslog server, perform the following steps:

**Procedure**

- **Step 1** Send syslog messages in EMBLEM format to a syslog server over UDP using port 514.

  ```
  logging host interface_name ip_address {tcp[/port] | udp[/port]} [format emblem]
  ```

  Example:

  ```
  ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
  ```

  The `format emblem` keyword enables EMBLEM format logging for the syslog server (UDP only). The `interface_name` argument specifies the interface through which you access the syslog server. The `ip_address` argument specifies the IP address of the syslog server. The `tcp[/port]` or `udp[/port]` keyword and argument pair specify that the ASA and ASASM should use TCP or UDP to send syslog messages to the syslog server.

  You can configure the ASA and ASASM to send data to a syslog server using either UDP or TCP, but not both. The default protocol is UDP if you do not specify a protocol.

  You can use multiple `logging host` commands to specify additional servers that would all receive syslog messages. If you configure two or more logging servers, make sure that you limit the logging severity level to warnings for all logging servers.

  If you specify TCP, the ASA or ASASM discovers when the syslog server fails and as a security protection, new connections through the ASA are blocked. If you specify UDP, the ASA or ASASM continues to allow new connections whether or not the syslog server is operational. Valid port values for either protocol are 1025 through 65535. The default UDP port is 514. The default TCP port is 1470.

  **Note** Sending syslogs over TCP is not supported on a standby ASA.
Generate Syslog Messages in EMBLEM Format to Other Output Destinations

To generate syslog messages in EMBLEM format to other output destinations, perform the following steps:

Procedure

Step 1: Send syslog messages in EMBLEM format to output destinations other than a syslog server, such as Telnet or SSH sessions.

    logging emblem

Example:

ciscoasa(config)# logging emblem

Change the Amount of Internal Flash Memory Available for Logs

To change the amount of internal flash memory available for logs, perform the following steps:

Procedure

Step 1: Specify the maximum amount of internal flash memory available for saving log files.

    logging flash-maximum-allocation kbytes

Example:

ciscoasa(config)# logging flash-maximum-allocation 1200

By default, the ASA can use up to 1 MB of internal flash memory for log data. The minimum amount of internal flash memory that must be free for the ASA and ASASM to save log data is 3 MB.

If a log file being saved to internal flash memory would cause the amount of free internal flash memory to fall below the configured minimum limit, the ASA or ASASM deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files have been deleted, free memory is still below the limit, the ASA or ASASM fails to save the new log file.

Step 2: Specify the minimum amount of internal flash memory that must be free for the ASA or ASASM to save a log file.

    logging flash-minimum-free kbytes

Example:

ciscoasa(config)# logging flash-minimum-free 4000
Configure the Logging Queue

To configure the logging queue, perform the following steps:

Procedure

**Step 1** Specify the number of syslog messages that the ASA and ASASM can hold in its queue before sending them to the configured output destination.

```
logging queue message_count
```

Example:

```
ciscoasa(config)# logging queue 300
```

The ASA and ASASM have a fixed number of blocks in memory that can be allocated for buffering syslog messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the syslog message queue and the number of syslog servers specified. The default queue size is 512 syslog messages. The queue size is limited only by block memory availability. Valid values are from 0 to 8192 messages, depending on the platform. If the logging queue is set to zero, the queue is the maximum configurable size (8192 messages).

Send All Syslog Messages in a Class to a Specified Output Destination

To send all syslog messages in a class to a specified output destination, perform the following steps:

Procedure

**Step 1** Override the configuration in the specified output destination command. For example, if you specify that messages at severity level 7 should go to the internal log buffer and that ha class messages at severity level 3 should go to the internal log buffer, then the latter configuration takes precedence.

```
logging class message_class (buffered | console | history | mail | monitor | trap) [severity_level]
```

Example:

```
ciscoasa(config)# logging class ha buffered alerts
```

The **buffered**, **history**, **mail**, **monitor**, and **trap** keywords specify the output destination to which syslog messages in this class should be sent. The **history** keyword enables SNMP logging. The **monitor** keyword enables Telnet and SSH logging. The **trap** keyword enables syslog server logging. Select one destination per command line entry. To specify that a class should go to more than one destination, enter a new command for each output destination.
Enable Secure Logging

To enable secure logging, perform the following steps:

Procedure

Step 1

Enable secure logging.

```
logging host interface_name syslog_ip [tcp/port | udp/port] [format emblem] [secure]
```

Example:

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
```

The `interface_name` argument specifies the interface on which the syslog server resides. The `syslog_ip` argument specifies the IP address of the syslog server. The `port` argument specifies the port (TCP or UDP) that the syslog server listens to for syslog messages. The `tcp` keyword specifies that the ASA or ASASM should use TCP to send syslog messages to the syslog server. The `udp` keyword specifies that the ASA or ASASM should use UDP to send syslog messages to the syslog server. The `format emblem` keyword enables EMBLEM format logging for the syslog server. The `secure` keyword specifies that the connection to the remote logging host should use SSL/TLS for TCP only.

Note Secure logging does not support UDP; an error occurs if you try to use this protocol.

Include the Device ID in Non-EMBLEM Format Syslog Messages

To include the device ID in non-EMBLEM format syslog messages, perform the following steps:

Procedure

Step 1

Configure the ASA or ASASM to include a device ID in non-EMBLEM-format syslog messages. You can specify only one type of device ID for syslog messages.

```
logging device-id {cluster-id | context-name | hostname | ipaddress interface_name [system] | string text}
```

Example:

```
ciscoasa(config)# logging device-id hostname

ciscoasa(config)# logging device-id context-name
```

The `context-name` keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of `system`, and messages that originate in the admin context use the name of the admin context as the device ID.

Note In an ASA cluster, always use the master unit IP address for the selected interface.
Chapter 39      Logging

Configure Logging

The cluster-id keyword specifies the unique name in the boot configuration of an individual ASA unit in the cluster as the device ID. The hostname keyword specifies that the hostname of the ASA should be used as the device ID. The ipaddress interface_name keyword-argument pair specifies that the interface IP address specified as interface_name should be used as the device ID. If you use the ipaddress keyword, the device ID becomes the specified ASA interface IP address, regardless of the interface from which the syslog message is sent. In the cluster environment, the system keyword dictates that the device ID becomes the system IP address on the interface. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device. The string text keyword-argument pair specifies that the text string should be used as the device ID. The string can include as many as 16 characters.

You cannot use blank spaces or any of the following characters:

- & (ampersand)
- ‘ (single quote)
- " (double quote)
- < (less than)
- > (greater than)
- ? (question mark)

Note

If enabled, the device ID does not appear in EMBLEM-formatted syslog messages nor in SNMP traps.

Include the Date and Time in Syslog Messages

To include the date and time in syslog messages, perform the following steps:

Procedure

Step 1
Specify that syslog messages should include the date and time that they were generated.

logging timestamp

Example:
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT

To remove the date and time from syslog messages, enter the no logging timestamp command.

Disable a Syslog Message

To disable a specified syslog message, perform the following steps:

Procedure

Step 1
Prevent the ASA or ASASM from generating a particular syslog message.
Configure Logging

no logging message syslog_id

Example:
ciscoasa(config)# no logging message 113019

To reenable a disabled syslog message, enter the **logging message syslog_id** command (for example, **logging message 113019**). To reenable logging of all disabled syslog messages, enter the **clear configure logging disabled** command.

---

**Change the Severity Level of a Syslog Message**

To change the severity level of a syslog message, perform the following steps:

**Procedure**

**Step 1** Specify the severity level of a syslog message.

```
logging message syslog_id level severity_level
```

Example:
ciscoasa(config)# logging message 113019 level 5

To reset the severity level of a syslog message to its setting, enter the **no logging message syslog_id level severity_level** command (for example, **no logging message 113019 level 5**). To reset the severity level of all modified syslog messages to their settings, enter the **clear configure logging level** command.

---

**Limit the Rate of Syslog Message Generation**

To limit the rate of syslog message generation, perform the following steps:

**Procedure**

**Step 1** Apply a specified severity level (1 through 7) to a set of messages or to an individual message (not the destination) within a specified time period.

```
logging rate-limit {unlimited | {num [interval]}} message syslog_id | level severity_level
```

Example:
ciscoasa(config)# logging rate-limit 1000 600 level 6

Rate limits affect the volume of messages being sent to all configured destinations. To reset the logging rate limit to the default value, enter the **clear running-config logging rate-limit** command. To reset the logging rate limit, enter the **clear configure logging rate-limit** command.
Disabling Hidden Usernames in Syslogs

To hide usernames in syslogs when the username’s validity is unknown, perform the following steps:

**Procedure**

**Step 1**

Enter the following command:

`logging hide username`

Example:

`ciscoasa(config)# logging hide username`

The default is to hide usernames in syslogs when the username’s validity is unknown. To view these usernames, use the `no logging hide username` command.

Monitoring the Logs

See the following commands for monitoring logging status.

- **show logging**
  
  This command shows syslog messages, including the severity level.

  **Note**: The maximum number of syslog messages that are available to view is 1000, which is the default setting. The maximum number of syslog messages that are available to view is 2000.

- **show logging message**
  
  This command shows a list of syslog messages with modified severity levels and disabled syslog messages.

- **show logging message message_ID**
  
  This command shows the severity level of a specific syslog message.

- **show logging queue**
  
  This command shows the logging queue and queue statistics.

- **show logging rate-limit**
  
  This command shows the disallowed syslog messages.

- **show running-config logging rate-limit**
  
  This command shows the current logging rate-limit setting.
Examples for Logging

The following example shows the logging information that displays for the `show logging` command:

ciscoasa(config)# show logging
Syslog logging: enabled
Facility: 16
Timestamp logging: disabled
Standby logging: disabled
Deny Conn when Queue Full: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: level errors, facility 16, 3607 messages logged
  Logging to infrastructure 10.1.2.3
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled

The following examples show how to control both whether a syslog message is enabled and the severity level of the specified syslog message:

ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1

ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503

ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503

ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3

ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
# History for Logging

## Table 39-2 History for Logging

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>7.0(1)</td>
<td>Provides ASA network logging information through various output destinations, and includes the option to view and save log files.</td>
</tr>
<tr>
<td>Rate limit</td>
<td>7.0(4)</td>
<td>Limits the rate at which syslog messages are generated. We introduced the following command: <code>logging rate-limit</code>.</td>
</tr>
<tr>
<td>Logging list</td>
<td>7.2(1)</td>
<td>Creates a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs). We introduced the following command: <code>logging list</code>.</td>
</tr>
<tr>
<td>Secure logging</td>
<td>8.0(2)</td>
<td>Specifies that the connection to the remote logging host should use SSL/TLS. This option is valid only if the protocol selected is TCP. We modified the following command: <code>logging host</code>.</td>
</tr>
<tr>
<td>Logging class</td>
<td>8.0(4), 8.1(1)</td>
<td>Added support for the ipaa event class of logging messages. We modified the following command: <code>logging class</code>.</td>
</tr>
<tr>
<td>Logging class and saved</td>
<td>8.2(1)</td>
<td>Added support for the dap event class of logging messages. We modified the following command: <code>logging class</code>. Added support to clear the saved logging buffers (ASDM, internal, FTP, and flash). We introduced the following command: <code>clear logging queue bufferwrap</code>.</td>
</tr>
<tr>
<td>logging buffers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password encryption</td>
<td>8.3(1)</td>
<td>Added support for password encryption. We modified the following command: <code>logging ftp server</code>.</td>
</tr>
<tr>
<td>Log viewers</td>
<td>8.3(1)</td>
<td>The source and destination IP addresses were added to the log viewers.</td>
</tr>
</tbody>
</table>
### History for Logging (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced logging and connection blocking</td>
<td>8.3(2)</td>
<td>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. This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommended allowing connections when syslog messages cannot be sent or received. To allow connections, continue to use the <code>logging permit-hostdown</code> command. We modified the following command: <code>show logging</code>. We introduced the following syslog messages: 414005, 414006, 414007, and 414008.</td>
</tr>
<tr>
<td>Syslog message filtering and sorting</td>
<td>8.4(1)</td>
<td>Support has been added for the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Syslog message filtering based on multiple text strings that correspond to various columns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Creation of custom filters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Column sorting of messages. For detailed information, see the ASDM configuration guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following screens:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring &gt; Logging &gt; Real-Time Log Viewer &gt; View.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring &gt; Logging &gt; Log Buffer Viewer &gt; View.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This feature interoperates with all ASA versions.</td>
</tr>
<tr>
<td>Clustering</td>
<td>9.0(1)</td>
<td>Added support for syslog message generation in a clustering environment on the ASA 5580 and 5585-X.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following command: <code>logging device-id</code>.</td>
</tr>
<tr>
<td>Hidden usernames in syslogs</td>
<td>9.3(3)</td>
<td>You can now hide usernames in syslogs when the username’s validity is unknown.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We introduced the <code>logging hide username</code> command. To view these usernames, use the <code>no logging hide username</code> command.</td>
</tr>
</tbody>
</table>
SNMP

This chapter describes how to configure Simple Network Management Protocol (SNMP) to monitor the Cisco ASA.

- About SNMP, page 40-1
- Guidelines for SNMP, page 40-20
- Configure SNMP, page 40-22
- Examples for SNMP, page 40-32
- Monitoring SNMP, page 40-31
- History for SNMP, page 40-33

About SNMP

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices and is part of the TCP/IP protocol suite. The ASA, ASAv, and ASASM provide support for network monitoring using SNMP Versions 1, 2c, and 3, and support the use of all three versions simultaneously. The SNMP agent running on the ASA interface lets you monitor the ASA and ASASM through network management systems (NMSs), such as HP OpenView. The ASA, ASAv, and ASASM support SNMP read-only access through issuance of a GET request. SNMP write access is not allowed, so you cannot make changes with SNMP. In addition, the SNMP SET request is not supported.

You can configure the ASA, ASAv, and ASASM to send traps, which are unsolicited messages from the managed device to the management station for certain events (event notifications) to an NMS, or you can use the NMS to browse the Management Information Bases (MIBs) on the ASA. MIBs are a collection of definitions, and the ASA, ASAv, and ASASM maintain a database of values for each definition. Browsing a MIB means issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the NMS to determine values.

The ASA, ASAv, and ASASM have an SNMP agent that notifies designated management stations if events occur that are predefined to require a notification, for example, when a link in the network goes up or down. The notification it sends includes an SNMP OID, which identifies itself to the management stations. The ASA, ASAv, or ASASM SNMP agent also replies when a management station asks for information.
SNMP Terminology

Table 40-1 lists the terms that are commonly used when working with SNMP.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>The SNMP server running on the ASA. The SNMP agent has the following features:</td>
</tr>
<tr>
<td></td>
<td>• Responds to requests for information and actions from the network management station.</td>
</tr>
<tr>
<td></td>
<td>• Controls access to its Management Information Base, the collection of objects that the SNMP manager can view or change.</td>
</tr>
<tr>
<td></td>
<td>• Does not allow SET operations.</td>
</tr>
<tr>
<td>Browsing</td>
<td>Monitoring the health of a device from the network management station by polling required information from the SNMP agent on the device. This activity may include issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the network management station to determine values.</td>
</tr>
<tr>
<td>Management Information Bases (MIBs)</td>
<td>Standardized data structures for collecting information about packets, connections, buffers, failovers, and so on. MIBs are defined by the product, protocols, and hardware standards used by most network devices. SNMP network management stations can browse MIBs and request specific data or events be sent as they occur.</td>
</tr>
<tr>
<td>Network management stations (NMSs)</td>
<td>The PCs or workstations set up to monitor SNMP events and manage devices, such as the ASA, ASAv, and ASASM.</td>
</tr>
<tr>
<td>Object identifier (OID)</td>
<td>The system that identifies a device to its NMS and indicates to users the source of information monitored and displayed.</td>
</tr>
<tr>
<td>Trap</td>
<td>Predefined events that generate a message from the SNMP agent to the NMS. Events include alarm conditions such as linkup, linkdown, coldstart, warmstart, authentication, or syslog messages.</td>
</tr>
</tbody>
</table>

MIBs and Traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. A trap reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. SNMP traps are compiled into the ASA, ASAv or ASASM software.

If needed, you can also download RFCs, standard MIBs, and standard traps from the following locations:

http://www.ietf.org/

Download a complete list of Cisco MIBs, traps, and OIDs from the following location:


In addition, download Cisco OIDs by FTP from the following location:

In software versions 7.2(1), 8.0(2), and later, the interface information accessed through SNMP refreshes about every 5 seconds. As a result, we recommend that you wait for at least 5 seconds between consecutive polls.

Not all OIDs in MIBs are supported. To obtain a list of the supported SNMP MIBs and OIDs for a specific ASA or ASASM, enter the following command:

ciscoasa(config)# show snmp-server oidlist

Although the oidlist keyword does not appear in the options list for the show snmp-server command help, it is available. However, this command is for Cisco TAC use only. Contact the Cisco TAC before using this command.

The following is sample output from the show snmp-server oidlist command:

ciscoasa(config)# show snmp-server oidlist
[0]  1.3.6.1.2.1.1.1.  sysDescr
[1]  1.3.6.1.2.1.1.2.  sysObjectID
[2]  1.3.6.1.2.1.1.3.  sysUpTime
[3]  1.3.6.1.2.1.1.4.  sysContact
[4]  1.3.6.1.2.1.1.5.  sysName
[5]  1.3.6.1.2.1.1.6.  sysLocation
[6]  1.3.6.1.2.1.1.7.  sysServices
[7]  1.3.6.1.2.1.2.1.  ifNumber
[8]  1.3.6.1.2.1.2.1.1.  ifIndex
[9]  1.3.6.1.2.1.2.1.2.  ifDescr
[10] 1.3.6.1.2.1.2.1.3.  ifType
[11] 1.3.6.1.2.1.2.1.4.  ifMtu
[12] 1.3.6.1.2.1.2.1.5.  ifSpeed
[13] 1.3.6.1.2.1.2.1.6.  ifPhysAddress
[14] 1.3.6.1.2.1.2.1.7.  ifAdminStatus
[15] 1.3.6.1.2.1.2.1.8.  ifOperStatus
[16] 1.3.6.1.2.1.2.1.9.  ifLastChange
[17] 1.3.6.1.2.1.2.1.10.  ifInOctets
[18] 1.3.6.1.2.1.2.1.11.  ifInUcastPkts
[19] 1.3.6.1.2.1.2.1.12.  ifInNUcastPkts
[20] 1.3.6.1.2.1.2.1.13.  ifInDiscards
[21] 1.3.6.1.2.1.2.1.14.  ifInErrors
[22] 1.3.6.1.2.1.2.1.15.  ifOutOctets
[23] 1.3.6.1.2.1.2.1.16.  ifOutUcastPkts
[24] 1.3.6.1.2.1.2.1.17.  ifOutNUcastPkts
[25] 1.3.6.1.2.1.2.1.18.  ifOutDiscards
[26] 1.3.6.1.2.1.2.1.19.  ifOutErrors
[27] 1.3.6.1.2.1.2.1.20.  ifOutQLen
[28] 1.3.6.1.2.1.2.1.21.  ifSpecific
[29] 1.3.6.1.2.1.2.1.22.  ipForwarding
[30] 1.3.6.1.2.1.4.20.1.1.  ipAdEntAddr
[31] 1.3.6.1.2.1.4.20.1.2.  ipAdEntIfIndex
[32] 1.3.6.1.2.1.4.20.1.3.  ipAdEntNetMask
[33] 1.3.6.1.2.1.4.20.1.4.  ipAdEntBcastAddr
[34] 1.3.6.1.2.1.4.20.1.5.  ipAdEntRessmSize
[35] 1.3.6.1.2.1.11.1.  snmpInPkts
[36] 1.3.6.1.2.1.11.2.  snmpOutPkts
[37] 1.3.6.1.2.1.11.3.  snmpInBadVersions
[38] 1.3.6.1.2.1.11.4.  snmpInBadCommunityNames
[39] 1.3.6.1.2.1.11.5.  snmpInBadCommunityUses
[40] 1.3.6.1.2.1.11.6.  snmpInASNParseErrs
[41] 1.3.6.1.2.1.11.8.  snmpInTooBigs
About SNMP

[42] 1.3.6.1.2.1.11.9.  snmpInNoSuchNames
[43] 1.3.6.1.2.1.11.10. snmpInBadValues
[44] 1.3.6.1.2.1.11.11. snmpInReadOnlys
[45] 1.3.6.1.2.1.11.12. snmpInGenErrs
[46] 1.3.6.1.2.1.11.13. snmpInTotalReqVars
[47] 1.3.6.1.2.1.11.14. snmpInTotalSetVars
[48] 1.3.6.1.2.1.11.15. snmpInGetRequests
[49] 1.3.6.1.2.1.11.16. snmpInGetNexts
[50] 1.3.6.1.2.1.11.17. snmpInSetRequests
[51] 1.3.6.1.2.1.11.18. snmpInGetResponses
[52] 1.3.6.1.2.1.11.19. snmpInTraps
[53] 1.3.6.1.2.1.11.20. snmpOutTooBigs
[54] 1.3.6.1.2.1.11.21. snmpOutNoSuchNames
[55] 1.3.6.1.2.1.11.22. snmpOutBadValues
[56] 1.3.6.1.2.1.11.24. snmpOutGenErrs
[57] 1.3.6.1.2.1.11.25. snmpOutGetRequests
[58] 1.3.6.1.2.1.11.26. snmpOutGetNexts
[59] 1.3.6.1.2.1.11.27. snmpOutSetRequests
[60] 1.3.6.1.2.1.11.28. snmpOutGetResponses
[61] 1.3.6.1.2.1.11.29. snmpOutTraps
[62] 1.3.6.1.2.1.11.30. snmpEnableAuthenTraps
[63] 1.3.6.1.2.1.11.31. snmpSilentDrops
[64] 1.3.6.1.2.1.11.32. snmpProxyDrops
[65] 1.3.6.1.2.1.31.1.1.1.1. ifName
[66] 1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67] 1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68] 1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69] 1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70] 1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets

SNMP Object Identifiers

Each Cisco system-level product has an SNMP object identifier (OID) for use as a MIB-II sysObjectID. The CISCO-PRODUCTS-MIB includes the OIDs that can be reported in the sysObjectID object in the SNMPv2-MIB. You can use this value to identify the model type. Table 40-2 lists the sysObjectID OIDs for ASA models.

Table 40-2  SNMP Object Identifiers

<table>
<thead>
<tr>
<th>Product Identifier</th>
<th>sysObjectID</th>
<th>Model Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506 Adaptive Security Appliance</td>
<td>ciscoASA5506 (ciscoProducts 2114)</td>
<td>ASA 5506-X</td>
</tr>
<tr>
<td>ASA 5506 Adaptive Security Appliance Security Context</td>
<td>ciscoASA5506sc (ciscoProducts 2115)</td>
<td>ASA 5506-X security context</td>
</tr>
<tr>
<td>ASA 5506 Adaptive Security Appliance System Context</td>
<td>ciscoASA5506sy (ciscoProducts 2116)</td>
<td>ASA 5506-X system context</td>
</tr>
<tr>
<td>ASA 5506 Adaptive Security Appliance with No Payload Encryption</td>
<td>ciscoASA5506K7 (ciscoProducts 2123)</td>
<td>ASA 5506-X Adaptive Security Appliance with No Payload Encryption</td>
</tr>
<tr>
<td>Object Description</td>
<td>Object Identifier</td>
<td>Context Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ASA 5506 Adaptive Security Appliance System Context with No Payload Encryption</td>
<td>ciscoASA5506K7sy (ciscoProducts 2125)</td>
<td>ASA 5506-X Adaptive Security Appliance System Context with No Payload Encryption</td>
</tr>
<tr>
<td>ASA5585-SSP10</td>
<td>ciscoASA5585Ssp10 (ciscoProducts 1194)</td>
<td>ASA 5585-X SSP-10</td>
</tr>
<tr>
<td>ASA5585-SSP20</td>
<td>ciscoASA5585Ssp20 (ciscoProducts 1195)</td>
<td>ASA 5585-X SSP-20</td>
</tr>
<tr>
<td>ASA5585-SSP40</td>
<td>ciscoASA5585Ssp40 (ciscoProducts 1196)</td>
<td>ASA 5585-X SSP-40</td>
</tr>
<tr>
<td>ASA5585-SSP60</td>
<td>ciscoASA5585Ssp60 (ciscoProducts 1197)</td>
<td>ASA 5585-X SSP-60</td>
</tr>
<tr>
<td>ASA5585-SSP10 security context</td>
<td>ciscoASA5585Ssp10sc (ciscoProducts 1198)</td>
<td>ASA 5585-X SSP-10 security context</td>
</tr>
<tr>
<td>ASA5585-SSP20 security context</td>
<td>ciscoASA5585Ssp20sc (ciscoProducts 1199)</td>
<td>ASA 5585-X SSP-20 security context</td>
</tr>
<tr>
<td>ASA5585-SSP40 security context</td>
<td>ciscoASA5585Ssp40sc (ciscoProducts 1200)</td>
<td>ASA 5585-X SSP-40 security context</td>
</tr>
<tr>
<td>ASA5585-SSP60 security context</td>
<td>ciscoASA5585Ssp60sc (ciscoProducts 1201)</td>
<td>ASA 5585-X SSP-60 security context</td>
</tr>
<tr>
<td>ASA5585-SSP10 system context</td>
<td>ciscoASA5585Ssp10sy (ciscoProducts 1202)</td>
<td>ASA 5585-X SSP-10 system context</td>
</tr>
<tr>
<td>ASA5585-SSP20 system context</td>
<td>ciscoASA5585Ssp20sy (ciscoProducts 1203)</td>
<td>ASA 5585-X SSP-20 system context</td>
</tr>
<tr>
<td>ASA5585-SSP40 system context</td>
<td>ciscoASA5585Ssp40sy (ciscoProducts 1204)</td>
<td>ASA 5585-X SSP-40 system context</td>
</tr>
<tr>
<td>ASA5585-SSP60 system context</td>
<td>ciscoASA5585Ssp60sy (ciscoProducts 1205)</td>
<td>ASA 5585-X SSP-60 system context</td>
</tr>
<tr>
<td>ASA Services Module for Catalyst switches/7600 routers</td>
<td>ciscoAsaSm1 (ciscoProducts 1277)</td>
<td>Adaptive Security Appliance (ASA) Services Module for Catalyst switches/7600 routers</td>
</tr>
<tr>
<td>ASA Services Module for Catalyst switches/7600 routers security context</td>
<td>ciscoAsaSm1sc (ciscoProducts 1275)</td>
<td>Adaptive Security Appliance (ASA) Services Module for Catalyst switches/7600 routers security context</td>
</tr>
<tr>
<td>ASA Services Module for Catalyst switches/7600 routers security context with No Payload Encryption</td>
<td>ciscoAsaSm1K7sc (ciscoProducts 1334)</td>
<td>Adaptive Security Appliance (ASA) Services Module for Catalyst switches/7600 routers security context with No Payload Encryption</td>
</tr>
<tr>
<td>ASA Services Module for Catalyst switches/7600 routers system context</td>
<td>ciscoAsaSm1sy (ciscoProducts 1276)</td>
<td>Adaptive Security Appliance (ASA) Services Module for Catalyst switches/7600 routers system context</td>
</tr>
<tr>
<td>ASA Services Module for Catalyst switches system context/7600 routers with No Payload Encryption</td>
<td>ciscoAsaSm1K7sy (ciscoProducts 1335)</td>
<td>Adaptive Security Appliance (ASA) Services Module for Catalyst switches/7600 routers system context with No Payload Encryption</td>
</tr>
</tbody>
</table>
Table 40-2  SNMP Object Identifiers (continued)

<table>
<thead>
<tr>
<th>ASA Services Module for Catalyst switches/7600 routers system context with No Payload Encryption</th>
<th>ciscoAsaSm1K7 (ciscoProducts 1336)</th>
<th>Adaptive Security Appliance (ASA) Services Module for Catalyst switches/7600 routers with No Payload Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5512</td>
<td>ciscoASA5512 (ciscoProducts 1407)</td>
<td>ASA 5512 Adaptive Security Appliance</td>
</tr>
<tr>
<td>ASA 5525</td>
<td>ciscoASA5525 (ciscoProducts 1408)</td>
<td>ASA 5525 Adaptive Security Appliance</td>
</tr>
<tr>
<td>ASA 5545</td>
<td>ciscoASA5545 (ciscoProducts 1409)</td>
<td>ASA 5545 Adaptive Security Appliance</td>
</tr>
<tr>
<td>ASA 5555</td>
<td>ciscoASA5555 (ciscoProducts 1410)</td>
<td>ASA 5555 Adaptive Security Appliance</td>
</tr>
<tr>
<td>ASA 5512 Security Context</td>
<td>ciscoASA5512sc (ciscoProducts 1411)</td>
<td>ASA 5512 Adaptive Security Appliance Security Context</td>
</tr>
<tr>
<td>ASA 5525 Security Context</td>
<td>ciscoASA5525sc (ciscoProducts 1412)</td>
<td>ASA 5525 Adaptive Security Appliance Security Context</td>
</tr>
<tr>
<td>ASA 5545 Security Context</td>
<td>ciscoASA5545sc (ciscoProducts 1413)</td>
<td>ASA 5545 Adaptive Security Appliance Security Context</td>
</tr>
<tr>
<td>ASA 5555 Security Context</td>
<td>ciscoASA5555sc (ciscoProducts 1414)</td>
<td>ASA 5555 Adaptive Security Appliance Security Context</td>
</tr>
<tr>
<td>ASA 5512 System Context</td>
<td>ciscoASA5512sy (ciscoProducts 1415)</td>
<td>ASA 5512 Adaptive Security Appliance System Context</td>
</tr>
<tr>
<td>ASA 5515 System Context</td>
<td>ciscoASA5515sy (ciscoProducts 1416)</td>
<td>ASA 5515 Adaptive Security Appliance System Context</td>
</tr>
<tr>
<td>ASA 5525 System Context</td>
<td>ciscoASA5525sy (ciscoProducts 1417)</td>
<td>ASA 5525 Adaptive Security Appliance System Context</td>
</tr>
<tr>
<td>ASA 5545 System Context</td>
<td>ciscoASA5545sy (ciscoProducts 1418)</td>
<td>ASA 5545 Adaptive Security Appliance System Context</td>
</tr>
<tr>
<td>ASA 5555 System Context</td>
<td>ciscoASA5555sy (ciscoProducts 1419)</td>
<td>ASA 5555 Adaptive Security Appliance System Context</td>
</tr>
<tr>
<td>ASA 5515 Security Context</td>
<td>ciscoASA5515sc (ciscoProducts 1420)</td>
<td>ASA 5515 Adaptive Security Appliance System Context</td>
</tr>
<tr>
<td>ASA 5515</td>
<td>ciscoASA5515 (ciscoProducts 1421)</td>
<td>ASA 5515 Adaptive Security Appliance</td>
</tr>
<tr>
<td>ASAv</td>
<td>ciscoASAv (ciscoProducts 1902)</td>
<td>Cisco Adaptive Security Virtual Appliance (ASAv)</td>
</tr>
<tr>
<td>ASAv System Context</td>
<td>ciscoASAvsy (ciscoProducts 1903)</td>
<td>Cisco Adaptive Security Virtual Appliance (ASAv) System Context</td>
</tr>
</tbody>
</table>
Physical Vendor Type Values

Each Cisco chassis or standalone system has a unique type number for SNMP use. The entPhysicalVendorType OIDs are defined in the CISCO-ENTITY-VENDORTYPE-OID-MIB. This value is returned in the entPhysicalVendorType object from the ASA, ASAv, or ASASM SNMP agent. You can use this value to identify the type of component (module, power supply, fan, sensors, CPU, and so on). Table 40-3 lists the physical vendor type values for the ASA and ASASM models.

Table 40-3 Physical Vendor Type Values

<table>
<thead>
<tr>
<th>Item</th>
<th>entPhysicalVendorType OID Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA Services Module for Catalyst switches/7600 routers</td>
<td>cevCat6kWsSvcAsaSm1 (cevModuleCat6000Type 169)</td>
</tr>
<tr>
<td>ASA Services Module for Catalyst switches/7600 routers with No Payload Encryption</td>
<td>cevCat6kWsSvcAsaSm1K7 (cevModuleCat6000Type 186)</td>
</tr>
<tr>
<td>Accelerator for 5506 Adaptive Security Appliance</td>
<td>cevAcceleratorAsa5506 (cevOther 10)</td>
</tr>
<tr>
<td>Accelerator for 5506 with No Payload Encryption Adaptive Security Appliance</td>
<td>cevAcceleratorAsa5506K7 (cevOther 13)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5506 Chassis</td>
<td>cevChassisAsa5506 (cevChassis 1600)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5506 Chassis with No Payload Encryption</td>
<td>cevChassisAsa5506K7 (cevChassis 1603)</td>
</tr>
<tr>
<td>Central Processing Unit for 5506 Adaptive Security Appliance</td>
<td>cevCpuAsa5506 (cevModuleCpuType 312)</td>
</tr>
<tr>
<td>Central Processing Unit for 5506 with No Payload Encryption Adaptive Security Appliance</td>
<td>cevCpuAsa5506K7 (cevModuleCpuType 315)</td>
</tr>
<tr>
<td>cevModuleASA5506 Type chassis</td>
<td>cevModuleASA5506Type (cevModule 107)</td>
</tr>
<tr>
<td>5506 Adaptive Security Appliance Field-Replaceable Solid State Drive</td>
<td>cevModuleAsa5506SSD (cevModuleASA5506Type 1)</td>
</tr>
<tr>
<td>5506 with No Payload Encryption Adaptive Security Appliance Field-Replaceable Solid State Drive</td>
<td>cevModuleAsa5506K7SSD (cevModuleASA5506Type 3)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for 5506 Adaptive Security Appliance</td>
<td>cevSensorAsa5506CpuTempSensor (cevSensor 164)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for 5506 with No Payload Encryption Adaptive Security Appliance</td>
<td>cevSensorAsa5506K7CpuTempSensor (cevSensor 167)</td>
</tr>
<tr>
<td>Accelerator Temperature Sensor for 5506 Adaptive Security Appliance</td>
<td>cevSensorAsa5506AcceleratorTempSensor (cevSensor 169)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for 5506 Adaptive Security Appliance</td>
<td>cevSensorAsa5506ChassisTempSensor (cevSensor 174)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for 5506 with No Payload Encryption Adaptive Security Appliance</td>
<td>cevSensorAsa5506K7ChassisTempSensor (cevSensor 177)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5512 Adaptive Security Appliance</td>
<td>cevChassisASA5512 (cevChassis 1113)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5512 Adaptive Security Appliance with No Payload Encryption</td>
<td>cevChassisASA5512K7 (cevChassis 1108 )</td>
</tr>
</tbody>
</table>
## Table 40-3  Physical Vendor Type Values (continued)

<table>
<thead>
<tr>
<th>Model Description</th>
<th>Vendor Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5515 Adaptive Security Appliance</td>
<td>cevChassisASA5515 (cevChassis 1114)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5515 Adaptive Security Appliance with No Payload Encryption</td>
<td>cevChassisASA5515K7 (cevChassis 1109 )</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5525 Adaptive Security Appliance</td>
<td>cevChassisASA5525 (cevChassis 1115)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5525 Adaptive Security Appliance with No Payload Encryption</td>
<td>cevChassisASA5525K7 (cevChassis 1110 )</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5545 Adaptive Security Appliance</td>
<td>cevChassisASA5545 (cevChassis 1116)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5545 Adaptive Security Appliance with No Payload Encryption</td>
<td>cevChassisASA5545K7 (cevChassis 1111 )</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5555 Adaptive Security Appliance</td>
<td>cevChassisASA5555 (cevChassis 1117)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5555 Adaptive Security Appliance with No Payload Encryption</td>
<td>cevChassisASA5555K7 (cevChassis 1112 )</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5512</td>
<td>cevCpuAsa5512 (cevModuleCpuType 229)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5512 with no Payload Encryption</td>
<td>cevCpuAsa5512K7 (cevModuleCpuType 224)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5515</td>
<td>cevCpuAsa5515 (cevModuleCpuType 230)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5515 with no Payload Encryption</td>
<td>cevCpuAsa5515K7 (cevModuleCpuType 225)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5525</td>
<td>cevCpuAsa5525 (cevModuleCpuType 231)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5525 with no Payload Encryption</td>
<td>cevCpuAsa5525K7 (cevModuleCpuType 226)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5545</td>
<td>cevCpuAsa5545 (cevModuleCpuType 232)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5545 with no Payload Encryption</td>
<td>cevCpuAsa5545K7 (cevModuleCpuType 227)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5555</td>
<td>cevCpuAsa5555 (cevModuleCpuType 233)</td>
</tr>
<tr>
<td>Central Processing Unit for Cisco Adaptive Security Appliance 5555 with no Payload Encryption</td>
<td>cevCpuAsa5555K7 (cevModuleCpuType 228)</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-10</td>
<td>cevCpuAsa5585Ssp10 (cevModuleCpuType 204)</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-10 No Payload Encryption</td>
<td>cevCpuAsa5585Ssp10K7 (cevModuleCpuType 204)</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-20</td>
<td>cevCpuAsa5585Ssp20 (cevModuleCpuType 206)</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-20 No Payload Encryption</td>
<td>cevCpuAsa5585Ssp20K7 (cevModuleCpuType 207)</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-40</td>
<td>cevCpuAsa5585Ssp40 (cevModuleCpuType 208)</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-40 No Payload Encryption</td>
<td>cevCpuAsa5585Ssp40K7 (cevModuleCpuType 209)</td>
</tr>
<tr>
<td>Device Description</td>
<td>CEV Module ID</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-60</td>
<td>cevCpuAsa5585Ssp60 (cevModuleCpuType 210)</td>
</tr>
<tr>
<td>CPU for ASA 5585 SSP-60 No Payload Encryption</td>
<td>cevCpuAsa5585Ssp60K (cevModuleCpuType 211)</td>
</tr>
<tr>
<td>CPU for Cisco ASA Services Module for Catalyst switches/7600 routers</td>
<td>cevCpuAsaSm1 (cevModuleCpuType 222)</td>
</tr>
<tr>
<td>CPU for Cisco ASA Services Module with No Payload Encryption for Catalyst switches/7600 routers</td>
<td>cevCpuAsaSm1K7 (cevModuleCpuType 223)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5512</td>
<td>cevFanASA5512ChassisFan (cevFan 163)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5512 with No Payload Encryption</td>
<td>cevFanASA5512K7ChassisFan (cevFan 172)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5515</td>
<td>cevFanASA5515ChassisFan (cevFan 164)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5515 with No Payload Encryption</td>
<td>cevFanASA5515K7ChassisFan (cevFan 171)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5525</td>
<td>cevFanASA5525ChassisFan (cevFan 165)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5525 with No Payload Encryption</td>
<td>cevFanASA5525K7ChassisFan (cevFan 170)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5545</td>
<td>cevFanASA5545ChassisFan (cevFan 166)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevFanASA5545K7ChassisFan (cevFan 169)</td>
</tr>
<tr>
<td>Power Supply Fan in Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevFanASA5545K7PSFan (cevFan 161)</td>
</tr>
<tr>
<td>Power Supply Fan in Adaptive Security Appliance 5545</td>
<td>cevFanASA5545PSFan (cevFan 159)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5555</td>
<td>cevFanASA5555ChassisFan (cevFan 167)</td>
</tr>
<tr>
<td>Chassis Cooling Fan in Adaptive Security Appliance 5555 with No Payload Encryption</td>
<td>cevFanASA5555K7ChassisFan (cevFan 168)</td>
</tr>
<tr>
<td>Power Supply Fan in Adaptive Security Appliance 5555</td>
<td>cevFanASA5555PSFan (cevFan 160)</td>
</tr>
<tr>
<td>Power Supply Fan in Adaptive Security Appliance 5555 with No Payload Encryption</td>
<td>cevFanASA5555PSFanK7 (cevFan 162)</td>
</tr>
<tr>
<td>Power supply fan for ASA 5585-X</td>
<td>cevFanASA5585PSFan (cevFan 146)</td>
</tr>
<tr>
<td>10-Gigabit Ethernet interface</td>
<td>cevPort10GigEthernet (cevPort 315)</td>
</tr>
<tr>
<td>Gigabit Ethernet port</td>
<td>cevPortGe (cevPort 109)</td>
</tr>
<tr>
<td>Power Supply unit in Adaptive Security Appliance 5545</td>
<td>cevPowerSupplyASA5545PSInput (cevPowerSupply 323)</td>
</tr>
<tr>
<td>Power Supply unit in Adaptive Security Appliance 5555</td>
<td>cevPowerSupplyASA5555PSInput (cevPowerSupply 324)</td>
</tr>
<tr>
<td>Presence Sensor for Power Supply input in Adaptive Security Appliance 5555</td>
<td>cevPowerSupplyASA5555PSPresence (cevPowerSupply 322)</td>
</tr>
<tr>
<td>Power supply input for ASA 5585</td>
<td>cevPowerSupplyASA5585PSInput (cevPowerSupply 304)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5512 Chassis Fan sensor</td>
<td>cevSensorASA5512ChassisFanSensor (cevSensor 120)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5512</td>
<td>cevSensorASA5512ChassisTemp (cevSensor 107)</td>
</tr>
</tbody>
</table>
### Table 40-3 Physical Vendor Type Values (continued)

<table>
<thead>
<tr>
<th>Sensor Description</th>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5512</td>
<td>cevSensorASA5512CPUTemp (cevSensor 96)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5512 with No Payload Encryption Chassis Fan sensor</td>
<td>cevSensorASA5512K7ChassisFanSensor (cevSensor 125)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5512 with No Payload Encryption</td>
<td>cevSensorASA5512K7CPUTemp (cevSensor 102)</td>
</tr>
<tr>
<td>Sensor for Chassis Cooling Fan in Adaptive Security Appliance 5512</td>
<td>cevSensorASA5512PSFanSensor (cevSensor 119)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5515 Chassis Fan sensor</td>
<td>cevSensorASA5515ChassisFanSensor (cevSensor 121)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5515</td>
<td>cevSensorASA5515ChassisTemp (cevSensor 98)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5515</td>
<td>cevSensorASA5515CPUTemp (cevSensor 97)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5515 with No Payload Encryption Chassis Fan sensor</td>
<td>cevSensorASA5515K7ChassisFanSensor (cevSensor 126)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5515 with No Payload Encryption</td>
<td>cevSensorASA5515K7CPUTemp (cevSensor 103)</td>
</tr>
<tr>
<td>Sensor for Chassis Cooling Fan in Adaptive Security Appliance 5515</td>
<td>cevSensorASA5515PSFanSensor (cevSensor 118)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5525 Chassis Fan sensor</td>
<td>cevSensorASA5525ChassisFanSensor (cevSensor 122)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5525</td>
<td>cevSensorASA5525ChassisTemp (cevSensor 108)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5525</td>
<td>cevSensorASA5525CPUTemp (cevSensor 99)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5525 with No Payload Encryption Chassis Fan sensor</td>
<td>cevSensorASA5525K7ChassisFanSensor (cevSensor 127)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5525 with No Payload Encryption</td>
<td>cevSensorASA5525K7CPUTemp (cevSensor 104)</td>
</tr>
<tr>
<td>Sensor for Chassis Cooling Fan in Adaptive Security Appliance 5525 with No Payload Encryption</td>
<td>cevSensorASA5525K7PSFanSensor (cevSensor 114)</td>
</tr>
<tr>
<td>Sensor for Chassis Cooling Fan in Adaptive Security Appliance 5525</td>
<td>cevSensorASA5525PSFanSensor (cevSensor 117)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5545 Chassis Fan sensor</td>
<td>cevSensorASA5545ChassisFanSensor (cevSensor 123)</td>
</tr>
<tr>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5545</td>
<td>cevSensorASA5545ChassisTemp (cevSensor 109)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5545</td>
<td>cevSensorASA5545CPU Temp (cevSensor 100)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5545 with No Payload Encryption Chassis Fan sensor</td>
<td>cevSensorASA5545K7ChassisFanSensor (cevSensor 128)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevSensorASA5545K7ChassisTemp (cevSensor 90)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevSensorASA5545K7CPU Temp (cevSensor 105)</td>
</tr>
<tr>
<td>Sensor for Chassis Cooling Fan in Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevSensorASA5545K7PSFanSensor (cevSensor 113)</td>
</tr>
<tr>
<td>Presence Sensor for Power Supply input in Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevSensorASA5545K7PSPres ence (cevSensor 87)</td>
</tr>
<tr>
<td>Temperature Sensor for Power Supply Fan in Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevSensorASA5545K7PSTempSensor (cevSensor 94)</td>
</tr>
<tr>
<td>Sensor for Power Supply Fan in Adaptive Security Appliance 5545 with No Payload Encryption</td>
<td>cevSensorASA5545PSFanSensor (cevSensor 89)</td>
</tr>
<tr>
<td>Presence Sensor for Power Supply input in Adaptive Security Appliance 5545</td>
<td>cevSensorASA5545PSPresence (cevSensor 130)</td>
</tr>
<tr>
<td>Presence Sensor for Power Supply input in Adaptive Security Appliance 5555</td>
<td>cevSensorASA5545PSPresence (cevSensor 131)</td>
</tr>
<tr>
<td>Temperature Sensor for Power Supply Fan in Adaptive Security Appliance 5545</td>
<td>cevSensorASA5545PSTempSensor (cevSensor 92)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5555 Chassis Fan sensor</td>
<td>cevSensorASA5555ChassisFanSensor (cevSensor 124)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5555</td>
<td>cevSensorASA5555ChassisTemp (cevSensor 110)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5555</td>
<td>cevSensorASA5555CPU Temp (cevSensor 101)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA) 5555 with No Payload Encryption Chassis Fan sensor</td>
<td>cevSensorASA5555K7ChassisFanSensor (cevSensor 129)</td>
</tr>
<tr>
<td>Chassis Ambient Temperature Sensor for Cisco Adaptive Security Appliance 5555 with No Payload Encryption</td>
<td>cevSensorASA5555K7ChassisTemp (cevSensor 111)</td>
</tr>
<tr>
<td>Central Processing Unit Temperature Sensor for Cisco Adaptive Security Appliance 5555 with No Payload Encryption</td>
<td>cevSensorASA5555K7CPU Temp (cevSensor 106)</td>
</tr>
<tr>
<td>Sensor for Chassis Cooling Fan in Adaptive Security Appliance 5555 with No Payload Encryption</td>
<td>cevSensorASA5555K7PSFanSensor (cevSensor 112)</td>
</tr>
<tr>
<td>Presence Sensor for Power Supply input in Adaptive Security Appliance 5555 with No Payload Encryption</td>
<td>cevSensorASA5555K7PSPres ence (cevSensor 88)</td>
</tr>
<tr>
<td>Temperature Sensor for Power Supply Fan in Adaptive Security Appliance 5555 with No Payload Encryption</td>
<td>cevSensorASA5555K7PSTempSensor (cevSensor 95)</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Sensor for Power Supply Fan in Adaptive Security Appliance 5555</td>
<td>cevSensorASA5555PSFanSensor (cevSensor 91)</td>
</tr>
<tr>
<td>Temperature Sensor for Power Supply Fan in Adaptive Security Appliance 5555</td>
<td>cevSensorASA5555PSTempSensor (cevSensor 93)</td>
</tr>
<tr>
<td>Sensor for power supply fan for ASA 5585-X</td>
<td>cevSensorASA5585PSFanSensor (cevSensor 86)</td>
</tr>
<tr>
<td>Sensor for power supply input for ASA 5585-X</td>
<td>cevSensorASA5585PSInput (cevSensor 85)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-10</td>
<td>cevSensorASA5585SSp10CPUTemp (cevSensor 77)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-10 No Payload Encryption</td>
<td>cevSensorASA5585SSp10K7CPUTemp (cevSensor 78)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-20</td>
<td>cevSensorASA5585SSp20CPUTemp (cevSensor 79)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-20 No Payload Encryption</td>
<td>cevSensorASA5585SSp20K7CPUTemp (cevSensor 80)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-40</td>
<td>cevSensorASA5585SSp40CPUTemp (cevSensor 81)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-40 No Payload Encryption</td>
<td>cevSensorASA5585SSp40K7CPUTemp (cevSensor 82)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-60</td>
<td>cevSensorASA5585SSp60CPUTemp (cevSensor 83)</td>
</tr>
<tr>
<td>CPU temperature sensor for ASA 5585 SSP-60 No Payload Encryption</td>
<td>cevSensorASA5585SSp60K7CPUTemp (cevSensor 84)</td>
</tr>
<tr>
<td>Adaptive Security Appliance 5555-X Field-Replaceable Solid State Drive</td>
<td>cevModuleASA5555XFRSSD (cevModuleCommonCards 396)</td>
</tr>
<tr>
<td>Adaptive Security Appliance 5545-X Field-Replaceable Solid State Drive</td>
<td>cevModuleASA5545XFRSSD (cevModuleCommonCards 397)</td>
</tr>
<tr>
<td>Adaptive Security Appliance 5525-X Field-Replaceable Solid State Drive</td>
<td>cevModuleASA5525XFRSSD (cevModuleCommonCards 398)</td>
</tr>
<tr>
<td>Adaptive Security Appliance 5515-X Field-Replaceable Solid State Drive</td>
<td>cevModuleASA5515XFRSSD (cevModuleCommonCards 399)</td>
</tr>
<tr>
<td>Adaptive Security Appliance 5512-X Field-Replaceable Solid State Drive</td>
<td>cevModuleASA5512XFRSSD (cevModuleCommonCards 400)</td>
</tr>
<tr>
<td>Cisco Adaptive Security Virtual Appliance</td>
<td>cevChassisASAv (cevChassis 1451)</td>
</tr>
</tbody>
</table>
# Supported Tables and Objects in MIBs

Table 40-4 lists the supported tables and objects for the specified MIBs.

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>Supported Tables and Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-ENHANCED-MEMPOOL-MIB</td>
<td>cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate,</td>
</tr>
<tr>
<td></td>
<td>cempMemPoolValid, cempMemPoolUsed, cempMemPoolFree, cempMemPoolUsedOvrflw, cempMemPoolHCUsed,</td>
</tr>
<tr>
<td></td>
<td>cempMemPoolFreeOvrflw, cempMemPoolHCFree</td>
</tr>
<tr>
<td>CISCO-ENTITY-SENSOR-EXT-MIB</td>
<td>ceSensorExtThresholdTable</td>
</tr>
<tr>
<td>Note</td>
<td>Not supported on the ASA Services Module for Catalyst 6500 switches/7600 routers.</td>
</tr>
<tr>
<td>CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB</td>
<td>ciscoL4L7ResourceLimitTable</td>
</tr>
<tr>
<td>CISCO-TRUSTSEC-SXP-MIB</td>
<td>ctsxSxpGlobalObjects, ctsxSxpConnectionObjects, ctsxSxpSgtObjects</td>
</tr>
<tr>
<td>Note</td>
<td>Not supported on the Cisco Adaptive Security Virtual Appliance (ASAv).</td>
</tr>
<tr>
<td>DISMAN-EVENT-MIB</td>
<td>mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable</td>
</tr>
<tr>
<td>DISMAN-EXPRESSION-MIB</td>
<td>expExpressionTable, expObjectTable, expValueTable</td>
</tr>
<tr>
<td>Note</td>
<td>Not supported on the ASA Services Module for Catalyst 6500 switches/7600 routers.</td>
</tr>
<tr>
<td>ENTITY-SENSOR-MIB</td>
<td>entPhySensorTable</td>
</tr>
<tr>
<td>Note</td>
<td>Not supported on the ASA Services Module for Catalyst 6500 switches/7600 routers.</td>
</tr>
<tr>
<td>NAT-MIB</td>
<td>natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom,</td>
</tr>
<tr>
<td></td>
<td>natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol,</td>
</tr>
<tr>
<td></td>
<td>natAddrMapAddrUsed, natAddrMapRowStatus</td>
</tr>
</tbody>
</table>
### Supported Traps (Notifications)

Table 40-5 lists the supported traps (notifications) and their associated MIBs.

<table>
<thead>
<tr>
<th>Trap and MIB Name</th>
<th>Varbind List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticationFailure (SNMPv2-MIB)</td>
<td>—</td>
<td>For SNMP Version 1 or 2, the community string provided in the SNMP request is incorrect. For SNMP Version 3, a report PDU is generated instead of a trap if the auth or priv passwords or usernames are incorrect. The <code>snmp-server enable traps snmp authentication</code> command is used to enable and disable transmission of these traps.</td>
</tr>
<tr>
<td>ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)</td>
<td>—</td>
<td>The <code>snmp-server enable traps config</code> command is used to enable transmission of this trap.</td>
</tr>
<tr>
<td>cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)</td>
<td>—</td>
<td>The <code>snmp-server enable traps entity fru-insert</code> command is used to enable this notification. This trap does not apply to the ASA 5506-X.</td>
</tr>
<tr>
<td>cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)</td>
<td>—</td>
<td>The <code>snmp-server enable traps entity fru-remove</code> command is used to enable this notification. This trap does not apply to the ASA 5506-X.</td>
</tr>
</tbody>
</table>
### Table 40-5 Supported Traps (Notifications) (continued)

<table>
<thead>
<tr>
<th>Trap Name (MIB)</th>
<th>Objects</th>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT -MIB)</td>
<td>ceSensorExtThresholdValue, entPhySensorValue, entPhySensorType, entPhysicalName</td>
<td>The `snmp-server enable traps entity [power-supply-failure</td>
</tr>
<tr>
<td>ceSensorExtThresholdValue, entPhySensorValue, entPhySensorType, entPhysicalName</td>
<td>The `snmp-server enable traps entity [power-supply-failure</td>
<td>fan-failure</td>
</tr>
<tr>
<td>ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT -MIB)</td>
<td>ceSensorExtThresholdValue, entPhySensorValue, entPhySensorType, entPhysicalName</td>
<td>The `snmp-server enable traps entity [power-supply-failure</td>
</tr>
<tr>
<td>cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)</td>
<td>cipSecTunLifeTime, cipSecTunLifeSize</td>
<td>The <code>snmp-server enable traps ipsec start</code> command is used to enable transmission of this trap.</td>
</tr>
</tbody>
</table>
Table 40-5  Supported Traps (Notifications) (continued)

<table>
<thead>
<tr>
<th>Trap Name</th>
<th>Trap Details</th>
<th>Command to Enable/Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR -MIB)</td>
<td>cipSecTunActiveTime</td>
<td>The <strong>snmp-server enable traps ipsec stop</strong> command is used to enable transmission of this trap.</td>
</tr>
<tr>
<td>ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)</td>
<td></td>
<td>The <strong>snmp-server enable traps config</strong> command is used to enable transmission of this trap.</td>
</tr>
<tr>
<td>ciscoRasTooManySessions (CISCO-REMOTE-ACCESS -MONITOR-MIB)</td>
<td>crasNumSessions, crasNumUsers, crasMaxSessionsSupportable, crasMaxUsersSupportable, crasThrMaxSessions</td>
<td>The <strong>snmp-server enable traps remote-access session-threshold-exceeded</strong> command is used to enable transmission of these traps.</td>
</tr>
<tr>
<td>clogMessageGenerated (CISCO-SYSLOG-MIB)</td>
<td>clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp</td>
<td>Syslog messages are generated. The value of the clogMaxSeverity object is used to decide which syslog messages are sent as traps. The <strong>snmp-server enable traps syslog</strong> command is used to enable and disable transmission of these traps.</td>
</tr>
<tr>
<td>clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE -LIMIT-MIB)</td>
<td>clrResourceLimitValueType, clrResourceLimitMax, clogOriginIDType, clogOriginID</td>
<td>The <strong>snmp-server enable traps connection-limit-reached</strong> command is used to enable transmission of the connection-limit-reached notification. The clogOriginID object includes the context name from which the trap originated.</td>
</tr>
<tr>
<td>coldStart (SNMPv2-MIB)</td>
<td></td>
<td>The SNMP agent has started. The <strong>snmp-server enable traps snmp coldstart</strong> command is used to enable and disable transmission of these traps.</td>
</tr>
<tr>
<td>cpmCPUrisingThreshold (CISCO-PROCESS-MIB)</td>
<td>cpmCPUrisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPUrisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev</td>
<td>The <strong>snmp-server enable traps cpu threshold rising</strong> command is used to enable transmission of the cpu threshold rising notification. The cpmCPUrisingThresholdPeriod object is sent with the other objects.</td>
</tr>
<tr>
<td>entConfigChange (ENTITY-MIB)</td>
<td></td>
<td>The <strong>snmp-server enable traps entity config-change fru-insert fru-remove</strong> command is used to enable this notification. <strong>Note</strong> This notification is only sent in multimode when a security context is created or removed.</td>
</tr>
<tr>
<td>linkDown (IF-MIB)</td>
<td>ifIndex, ifAdminStatus, ifOperStatus</td>
<td>The linkdown trap for interfaces. The <strong>snmp-server enable traps snmp linkdown</strong> command is used to enable and disable transmission of these traps.</td>
</tr>
</tbody>
</table>
### Interface Types and Examples

The interface types that produce SNMP traffic statistics include the following:

- **Logical**—Statistics collected by the software driver, which are a subset of physical statistics.
- **Physical**—Statistics collected by the hardware driver. Each physical named interface has a set of logical and physical statistics associated with it. Each physical interface may have more than one VLAN interface associated with it. VLAN interfaces only have logical statistics.

Note For a physical interface that has multiple VLAN interfaces associated with it, be aware that SNMP counters for ifInOctets and ifOutOctets OIDs match the aggregate traffic counters for that physical interface.

- **VLAN-only**—SNMP uses logical statistics for ifInOctets and ifOutOctets.

### Table 40-5 Supported Traps (Notifications) (continued)

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Parameters</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>linkUp (IF-MIB)</td>
<td>ifIndex, ifAdminStatus, ifOperStatus</td>
<td>The linkup trap for interfaces. The <code>snmp-server enable traps snmp linkup</code> command is used to enable and disable transmission of these traps.</td>
</tr>
<tr>
<td>mteTriggerFired (DISMAN-EVENT-MIB)</td>
<td>mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed</td>
<td>The <code>snmp-server enable traps memory-threshold</code> command is used to enable the memory threshold notification. The mteHotOID is set to cempMemPoolHCUsed. The cempMemPoolName and cempMemPoolHCUsed objects are sent with the other objects.</td>
</tr>
<tr>
<td>Note Not supported on the ASA Services Module for Catalyst 6500 switches/7600 routers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mteTriggerFired (DISMAN-EVENT-MIB)</td>
<td>mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName</td>
<td>The <code>snmp-server enable traps interface-threshold</code> command is used to enable the interface threshold notification. The entPhysicalName objects are sent with the other objects.</td>
</tr>
<tr>
<td>natPacketDiscard (NAT-MIB)</td>
<td>ifIndex</td>
<td>The <code>snmp-server enable traps nat packet-discard</code> command is used to enable the NAT packet discard notification. This notification is rate limited for 5 minutes and is generated when IP packets are discarded by NAT because mapping space is not available. The ifIndex gives the ID of the mapped interface.</td>
</tr>
<tr>
<td>warmStart (SNMPv2-MIB)</td>
<td>—</td>
<td>The <code>snmp-server enable traps snmp warmstart</code> command is used to enable and disable transmission of these traps.</td>
</tr>
</tbody>
</table>
The examples in Table 40-6 show the differences in SNMP traffic statistics. Example 1 shows the difference in physical and logical output statistics for the `show interface` command and the `show traffic` command. Example 2 shows output statistics for a VLAN-only interface for the `show interface` command and the `show traffic` command. The example shows that the statistics are close to the output that appears for the `show traffic` command.

### Table 40-6 SNMP Traffic Statistics for Physical and VLAN Interfaces

<table>
<thead>
<tr>
<th>Example 1</th>
<th>Example 2</th>
</tr>
</thead>
</table>
| ciscoasa# show interface GigabitEthernet3/2  
interface GigabitEthernet3/2  
    description fullt-mgmt  
    nameif mgmt  
    security-level 10  
    ip address 10.7.14.201 255.255.255.0  
    management-only  
  ciscoasa# show traffic  
(Condensed output)  
Physical Statistics  
  GigabitEthernet3/2:  
    received (in 121.760 secs)  
    36 packets  3428 bytes  
    0 pkts/sec  28 bytes/sec  
Logical Statistics  
  mgmt:  
    received (in 117.780 secs)  
    36 packets  2780 bytes  
    0 pkts/sec  23 bytes/sec  
| ciscoasa# show interface GigabitEthernet0/0.100  
interface GigabitEthernet0/0.100  
    vlan 100  
    nameif inside  
    security-level 100  
    ip address 10.7.1.101 255.255.255.0 standby 10.7.1.102  
ciscoasa# show traffic  
inside  
received (in 9921.450 secs)  
1977 packets  126528 bytes  
0 pkts/sec  12 bytes/sec  
transmitted (in 9921.450 secs)  
1978 packets  126556 bytes  
0 pkts/sec  12 bytes/sec  
| IfIndex of VLAN inside:  
  IF-MIB::ifDescr.9 = Adaptive Security Appliance ‘inside’ interface  
  IF-MIB::ifInOctets.9 = Counter32: 126318  

The following examples show the SNMP output statistics for the management interface and the physical interface. The ifInOctets value is close to the physical statistics output that appears in the `show traffic` command output but not to the logical statistics output.

IfIndex of the mgmt interface:  
IF-MIB::ifDescr.6 = Adaptive Security Appliance ‘mgmt’ interface

IfInOctets that corresponds to the physical interface statistics:  
IF-MIB::ifInOctets.6 = Counter32:3246

### SNMP Version 3 Overview

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or Version 2c. SNMP Versions 1 and 2c transmit data between the SNMP server and SNMP agent in clear text. SNMP Version 3 adds authentication and privacy options to secure protocol operations. In addition, this version controls access to the SNMP agent and MIB objects through the User-Based Security Model (USM) and View-Based Access Control Model (VACM). The ASA and ASASM also support the creation of SNMP groups and users, as well as hosts, which is required to enable transport authentication and encryption for secure SNMP communications.
Security Models

For configuration purposes, the authentication and privacy options are grouped together into security models. Security models apply to users and groups, which are divided into the following three types:

- **NoAuthPriv**—No Authentication and No Privacy, which means that no security is applied to messages.
- **AuthNoPriv**—Authentication but No Privacy, which means that messages are authenticated.
- **AuthPriv**—Authentication and Privacy, which means that messages are authenticated and encrypted.

SNMP Groups

An SNMP group is an access control policy to which users can be added. Each SNMP group is configured with a security model, and is associated with an SNMP view. A user within an SNMP group must match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique.

SNMP Users

SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SHA. The encryption algorithm options are DES, 3DES, and AES (which is available in 128, 192, and 256 versions). When you create a user, you must associate it with an SNMP group. The user then inherits the security model of the group.

SNMP Hosts

An SNMP host is an IP address to which SNMP notifications and traps are sent. To configure SNMP Version 3 hosts, along with the target IP address, you must configure a username, because traps are only sent to a configured user. SNMP target IP addresses and target parameter names must be unique on the ASA and ASA Services Module. Each SNMP host can have only one username associated with it. To receive SNMP traps, after you have added the `snmp-server host` command, make sure that you configure the user credentials on the NMS to match the credentials for the ASA and ASASM.

Implementation Differences Between the ASA, ASA Services Module, and the Cisco IOS Software

The SNMP Version 3 implementation in the ASA and ASASM differs from the SNMP Version 3 implementation in the Cisco IOS software in the following ways:

- The local-engine and remote-engine IDs are not configurable. The local engine ID is generated when the ASA or ASASM starts or when a context is created.
- No support exists for view-based access control, which results in unrestricted MIB browsing.
- Support is restricted to the following MIBs: USM, VACM, FRAMEWORK, and TARGET.
- You must create users and groups with the correct security model.
- You must remove users, groups, and hosts in the correct sequence.
- Use of the `snmp-server host` command creates an ASA, ASAv, or ASASM rule to allow incoming SNMP traffic.
SNMP Syslog Messaging

SNMP generates detailed syslog messages that are numbered 212nnn. Syslog messages indicate the status of SNMP requests, SNMP traps, SNMP channels, and SNMP responses from the ASA or ASASM to a specified host on a specified interface.

For detailed information about syslog messages, see the syslog messages guide.

Note

SNMP polling fails if SNMP syslog messages exceed a high rate (approximately 4000 per second).

Application Services and Third-Party Tools

For information about SNMP support, see the following URL:

For information about using third-party tools to walk SNMP Version 3 MIBs, see the following URL:

Guidelines for SNMP

This section includes guidelines and limitations that you should check before configuring SNMP.

Failover Guidelines

The SNMP client in each ASA, ASAv, or ASASM shares engine data with its peer. Engine data includes the engineID, engineBoots, and engineTime objects of the SNMP-FRAMEWORK-MIB. Engine data is written as a binary file to flash:/snmp/contextname.

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

- You must have Cisco Works for Windows or another SNMP MIB-II compliant browser to receive SNMP traps or browse a MIB.
- Does not support view-based access control, but the VACM MIB is available for browsing to determine default view settings.
- The ENTITY-MIB is not available in the non-admin context. Use the IF-MIB instead to perform queries in the non-admin context.
- Does not support SNMP Version 3 for the AIP SSM or AIP SSC.
- Does not support SNMP debugging.
- Does not support retrieval of ARP information.
- Does not support SNMP SET commands.
- When using NET-SNMP Version 5.4.2.1, only supports the encryption algorithm version of AES128. Does not support the encryption algorithm versions of AES256 or AES192.
• Changes to the existing configuration are rejected if the result places the SNMP feature in an inconsistent state.

• For SNMP Version 3, configuration must occur in the following order: group, user, host.

• Before a group is deleted, you must ensure that all users associated with that group are deleted.

• Before a user is deleted, you must ensure that no hosts are configured that are associated with that username.

• If users have been configured to belong to a particular group with a certain security model, and if the security level of that group is changed, you must do the following in this sequence:
  – Remove the users from that group.
  – Change the group security level.
  – Add users that belong to the new group.

• The creation of custom views to restrict user access to a subset of MIB objects is not supported.

• All requests and traps are available in the default Read/Notify View only.

• The connection-limit-reached trap is generated in the admin context. To generate this trap, you must have at least one SNMP server host configured in the user context in which the connection limit has been reached.

• You cannot query for the chassis temperature on the ASA 5585 SSP-40 (NPE).

• You can add up to 4000 hosts. However, only 128 of this number can be for traps.

• The total number of supported active polling destinations is 128.

• You can specify a network object to indicate the individual hosts that you want to add as a host group.

• You can associate more than one user with one host.

• You can specify overlapping network objects in different host-group commands. The values that you specify for the last host group take effect for the common set of hosts in the different network objects.

• If you delete a host group or hosts that overlap with other host groups, the hosts are set up again using the values that have been specified in the configured host groups.

• The values that the hosts acquire depend on the specified sequence that you use to run the commands.

• The limit on the message size that SNMP sends is 1472 bytes.

• Members of a cluster do not synchronize their SNMPv3 engine IDs. Because of this, each unit in the cluster should have a unique SNMPv3 user configuration.

**Troubleshooting Tips**

• To ensure that the SNMP process that receives incoming packets from the NMS is running, enter the following command:

  `ciscoasa(config)# show process | grep snmp`

• To capture syslog messages from SNMP and have them appear on the ASA, ASAv, or ASASM console, enter the following commands:

  `ciscoasa(config)# logging list snmp message 212001-212015`
  `ciscoasa(config)# logging console snmp`
Configure SNMP

This section describes how to configure SNMP.

Step 1  Enable the SNMP Agent and SNMP server. See Enable the SNMP Agent and SNMP Server, page 40-23.
Configure SNMP

**Step 2** Configure SNMP traps. See Configure SNMP Traps, page 40-23.

**Step 3** Configure SNMP Version 1 and 2c parameters or SNMP Version 3 parameters. See Configure Parameters for SNMP Version 1 or 2c, page 40-25 or Configure Parameters for SNMP Version 3, page 40-27.

---

**Enable the SNMP Agent and SNMP Server**

To enable the SNMP agent and SNMP server, perform the following steps:

**Procedure**

**Step 1** Enable the SNMP agent and SNMP server on the ASA, ASAv, or ASASM. By default, the SNMP server is enabled.

```
snmp-server enable
```

Example:

```
ciscoasa(config)# snmp-server enable
```

**Configure SNMP Traps**

To designate which traps that the SNMP agent generates and how they are collected and sent to NMSs, perform the following steps:

**Procedure**

**Step 1** Send individual traps, sets of traps, or all traps to the NMS.

```
```

Example:

```
ciscoasa(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
```

This command enables syslog messages to be sent as traps to the NMS. The default configuration has all SNMP standard traps enabled, as shown in the example. To disable these traps, use the no `snmp-server enable traps snmp` command. If you enter this command and do not specify a trap type, the default is the syslog trap. By default, the syslog trap is enabled. The default SNMP traps continue to be enabled with the syslog trap. You need to configure both the `logging history` command and the `snmp-server enable traps syslog` command to generate traps from the syslog MIB. To restore the default enabling of SNMP traps, use the `clear configure snmp-server` command. All other traps are disabled by default.
Traps available in the admin context only:

- connection-limit-reached
- entity
- memory-threshold

Traps generated through the admin context only for physically connected interfaces in the system context:

- interface-threshold

**Note**  The interface-threshold trap is not supported on the ASA Services Module for Catalyst 6500 switches/7600 routers.

All other traps are available in the admin and user contexts in single mode.

In multiple context mode, the fan-failure trap, the power-supply-failure trap, and the cpu-temperature trap are generated only from the admin context, and not the user contexts (applies only to the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X).

The accelerator-temperature threshold trap applies only to the ASA 5506-X.

The chassis-fan-failure trap does not apply to the ASA 5506-X.

The config trap enables the ciscoConfigManEvent notification and the ccmCLIRunningConfigChanged notification, which are generated after you have exited configuration mode.

The following traps do not apply to the ASA 5506-X: fan-failure, fru-insert, fru-remove, power-supply, power-supply-failure, power-supply-presence, and power-supply-temperature.

If the CPU usage is greater than the configured threshold value for the configured monitoring period, the cpu threshold rising trap is generated.

When the used system context memory reaches 80 percent of the total system memory, the memory-threshold trap is generated from the admin context. For all other user contexts, this trap is generated when the used memory reaches 80 percent of the total system memory in that particular context.

**Note**  SNMP does not monitor voltage sensors.

---

### Configure a CPU Usage Threshold

To configure a CPU usage threshold, perform the following steps:

**Procedure**

**Step 1**  Configure the threshold value for a high CPU threshold and the threshold monitoring period.

```
snmp cpu threshold rising threshold_value monitoring_period
```

Example:

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```
To clear the threshold value and monitoring period of the CPU utilization, use the `no` form of this command. If the `snmp cpu threshold rising` command is not configured, the default for the high threshold level is over 70 percent, and the default for the critical threshold level is over 95 percent. The default monitoring period is set to 1 minute.

You cannot configure the critical CPU threshold level, which is maintained at a constant 95 percent. Valid threshold values for a high CPU threshold range from 10 to 94 percent. Valid values for the monitoring period range from 1 to 60 minutes.

## Configure a Physical Interface Threshold

To configure the physical interface threshold, perform the following steps:

**Procedure**

**Step 1** Configure the threshold value for an SNMP physical interface.

```snmp interface threshold threshold_value```

Example:

```
ciscoasa(config)# snmp interface threshold 75%
```

To clear the threshold value for an SNMP physical interface, use the `no` form of this command. The threshold value is defined as a percentage of interface bandwidth utilization. Valid threshold values range from 30 to 99 percent. The default value is 70 percent.

The `snmp interface threshold` command is available only in the admin context.

Physical interface usage is monitored in single mode and multimode, and traps for physical interfaces in the system context are sent through the admin context. Only physical interfaces are used to compute threshold usage.

**Note** This command is not supported on the ASA Services Module for Catalyst 6500 switches/7600 routers.

## Configure Parameters for SNMP Version 1 or 2c

To configure parameters for SNMP Version 1 or 2c, perform the following steps:

**Procedure**

**Step 1** Specify the recipient of an SNMP notification, indicate the interface from which traps are sent, and identify the name and IP address of the NMS or SNMP manager that can connect to the ASA.

```snmp-server host {interface hostname | ip_address} [trap | poll] [community community-string] [version {1 | 2c username}] [udp-port port]```
Example:

ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2

ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

The **trap** keyword limits the NMS to receiving traps only. The **poll** keyword limits the NMS to sending requests (polling) only. By default, SNMP traps are enabled. By default, the UDP port is 162. The community string is a shared secret key between the ASA, ASAv, or ASASM and the NMS. The key is a case-sensitive value up to 32 alphanumeric characters long. Spaces are not permitted. The default community string is public. The ASA uses this key to determine whether or not the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the ASA and the management station with the same string. The ASA, ASAv, and ASASM use the specified string and do not respond to requests with an invalid community string. After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible. The encrypted community string is always generated by the ASA; you normally enter the clear text form.

**Note** If you downgrade from version 8.3(1) to a lower version of the ASA software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the **no key config-key password encryption** command, then save the results.

To receive traps after you have added the **snmp-server host** command, make sure that you configure the user on the NMS with the same credentials as the credentials configured on the ASA, ASAv, and ASASM.

**Step 2** Set the community string, which is for use only with SNMP Version 1 or 2c.

```
snmp-server community community-string
```

Example:

ciscoasa(config)# snmp-server community onceuponatime

**Step 3** Set the SNMP server location or contact information.

```
snmp-server [contact | location] text
```

Example:

ciscoasa(config)# snmp-server location building 42

ciscoasa(config)# snmp-server contact EmployeeA

The **text** argument specifies the name of the contact person or the ASA system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

**Step 4** Set the listening port for SNMP requests.

```
snmp-server listen-port lport
```

Example:

ciscoasa(config)# snmp-server lport 192

The **lport** argument is the port on which incoming requests are accepted. The default listening port is 161. The **snmp-server listen-port** command is only available in admin context, and is not available in the system context. If you configure the **snmp-server listen-port** command on a port that is currently in use, the following message appears:
Warning The UDP port port is in use by another feature. SNMP requests to the device will fail until
the snmp-server listen-port command is configured to use a different port.

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog
message %ASA-1-212001 if the port is still in use.

Configure Parameters for SNMP Version 3

To configure parameters for SNMP Version 3, perform the following steps:

Procedure

Step 1 Specify a new SNMP group, which is for use only with SNMP Version 3.

```
snmp-server group group-name v3 [auth | noauth | priv]
```

Example:
```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

When a community string is configured, two additional groups with the name that matches the
community string are autogenerated: one for the Version 1 security model and one for the Version 2
security model. For more information about security models, see Security Models, page 40-19. The auth
keyword enables packet authentication. The noauth keyword indicates no packet authentication or
encryption is being used. The priv keyword enables packet encryption and authentication. No default
values exist for the auth or priv keywords.

Step 2 Configure a new user for an SNMP group, which is for use only with SNMP Version 3.

```
snmp-server user username group-name {v3 [encrypted]} [auth {md5 | sha}] auth-password
{priv} [des | 3des | aes] [128 | 192 | 256] priv-password
```

Example:
```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword aes 128
mypassword

```

The username argument is the name of the user on the host that belongs to the SNMP agent. The
group-name argument is the name of the group to which the user belongs. The v3 keyword specifies that
the SNMP Version 3 security model should be used and enables the use of the encrypted, priv, and the
auth keywords. The encrypted keyword specifies the password in encrypted format. Encrypted
passwords must be in hexadecimal format. The auth keyword specifies which authentication level (md5
or sha) should be used. The priv keyword specifies the encryption level. No default values for the auth
or priv keywords, or default passwords exist. For the encryption algorithm, you can specify either the
des, 3des, or aes keyword. You can also specify which version of the AES encryption algorithm to use:
128, 192, or 256. The auth-password argument specifies the authentication user password. The
priv-password argument specifies the encryption user password.
Configure SNMP

Note
If you forget a password, you cannot recover it and you must reconfigure the user. You can specify a plain-text password or a localized digest. The localized digest must match the authentication algorithm selected for the user, which can be either MD5 or SHA. When the user configuration is displayed on the console or is written to a file (for example, the startup-configuration file), the localized authentication and privacy digests are always displayed instead of a plain-text password (see the second example). The minimum length for a password is 1 alphanumeric character; however, we recommend that you use at least 8 alphanumeric characters for security.

In clustering, you must manually update each clustered ASA with SNMPv3 users. You can do this by entering the `snmp-server user username group-name v3` command on the master unit with the `priv-password` option and `auth-password` option in their non-localized forms.

An error message appears to inform you that the SNMPv3 user commands will not be replicated during clustering replication or configuration. You may then configure SNMPv3 user and group commands on slave ASAs independently. This also means that existing SNMPv3 user and group commands are not cleared during replication, and you may enter SNMPv3 user and group commands on all slaves in the cluster. For example:

On a master unit using commands entered with keys that have already been localized:
```
ERROR: This command cannot be replicated because it contains localized keys.
```

On a slave unit during cluster replication (appears only if an `snmp-server user` commands exist in the configuration):
```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

Step 3
Specify the recipient of an SNMP notification. Indicate the interface from which traps are sent. Identify the name and IP address of the NMS or SNMP manager that can connect to the ASA.

```
snmp-server host interface (hostname | ip_address) [trap | poll] [community community-string] [version {1 | 2c | 3 username}] [udp-port port]
```

Example:
```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
```
```
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
```

The `trap` keyword limits the NMS to receiving traps only. The `poll` keyword limits the NMS to sending requests (polling) only. By default, SNMP traps are enabled. By default, the UDP port is 162. The community string is a shared secret key between the ASA and the NMS. The key is a case-sensitive value up to 32 alphanumeric characters. Spaces are not permitted. The default community-string is public. The ASA, ASAv, and ASASM use this key to determine whether the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the ASA, ASAv, or ASASM and the NMS with the same string. The ASA, ASAv, and ASASM use the specified string and do not respond to requests with an invalid community string. After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible. The encrypted community string is always generated by the ASA; you normally enter the clear text form.
If you downgrade from version 8.3(1) to a lower version of the ASA software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the `no key config-key password encryption` command, then save the results.

The `version` keyword specifies the SNMP trap version. The ASA does not support filtering based on SNMP requests (polling).

When SNMP Version 3 hosts are configured on the ASA, ASAv, and ASASM, a user must be associated with that host.

To receive traps after you have added the `snmp-server host` command, make sure that you configure the user on the NMS with the same credentials as the credentials configured on the ASA, ASAv, or ASASM. For more information about SNMP hosts, see SNMP Hosts, page 40-19.

**Step 4** Set the SNMP server location or contact information.

```
snmp-server [contact | location] text
```

Example:

```
ciscoasa(config)# snmp-server location building 42
```

```
ciscoasa(config)# snmp-server contact EmployeeA
```

The `text` argument specifies the name of the contact person or the ASA system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

**Step 5** Set the listening port for SNMP requests.

```
snmp-server listen-port lport
```

Example:

```
ciscoasa(config)# snmp-server listen-port 192
```

The `lport` argument is the port on which incoming requests are accepted. The default listening port is 161. The `snmp-server listen-port` command is only available in admin context, and is not available in the system context. If you configure the `snmp-server listen-port` command on a port that is currently in use, the following message appears:

**Warning** The UDP port `port` is in use by another feature. SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message `%ASA-1-212001` if the port is still in use.
Configure a Group of Users

To configure an SNMP user list with a group of specified users in it, perform the following steps:

Procedure

Step 1  Configure an SNMP user list.

```
snmp-server user-list list_name username user_name
```

Example:

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

The `listname` argument specifies the name of the user list, which may be up to 33 characters long. The `username user_name` keyword-argument pair specifies the users who may be configured in the user list.

You configure the users in the user list with the `snmp-server user username` command, which is available only if you are using SNMP Version 3. The user list must have more than one user in it and can be associated with a hostname or a range of IP addresses.

Associate Users with a Network Object

To associate a single user or a group of users in a user list with a network object, perform the following steps:

Procedure

Step 1  Associate a single user or a group of users in a user list with a network object.

```
snmp-server host-group net_obj_name [trap | poll] [community community-string] [version {1 | 2c | 3} {username | user-list list_name}] [udp-port port]
```

Example:

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1

ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c

ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1

ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

The `net_obj_name` argument specifies the interface network object name with which a user or group of users is associated. The `trap` keyword specifies that only traps can be sent, and that this host is not allowed to browse (poll). The `poll` keyword specifies that the host is allowed to browse (poll), but no traps can be sent. The `community` keyword specifies that a non-default string is required for requests from the NMS, or when generating traps sent to the NMS. You can use this keyword only for SNMP Version 1 or 2c. The `community-string` argument specifies the password-like community string that is sent with the notification or in a request from the NMS. The community string can have a maximum of 32 characters. The `version` keyword sets the SNMP notification version to Version 1, 2c, or 3 to use for sending traps. The `username` argument specifies the name of the user if you are using SNMP Version 3. The `user-list list_name` keyword-argument pair specifies the name of the user list. The `udp-port port`...
keyword-argument pair specifies that SNMP traps must be sent to an NMS host on a non-default port and sets the UDP port number of the NMS host. The default UDP port is 162. The default version is 1. SNMP traps are enabled by default.

---

**Monitoring SNMP**

See the following commands for monitoring SNMP:

- `show running-config snmp-server [default]`
  
  This command shows all SNMP server configuration information.

- `show running-config snmp-server group`
  
  This command shows SNMP group configuration settings.

- `show running-config snmp-server host`
  
  This command shows configuration settings used by SNMP to control messages and notifications sent to remote hosts.

- `show running-config snmp-server host-group`
  
  This command shows SNMP host group configurations.

- `show running-config snmp-server user`
  
  This command shows SNMP user-based configuration settings.

- `show running-config snmp-server user-list`
  
  This command shows SNMP user list configurations.

- `show snmp-server engineid`
  
  This command shows the ID of the SNMP engine configured.

- `show snmp-server group`
  
  This command shows the names of configured SNMP groups. If the community string has already been configured, two extra groups appear by default in the output. This behavior is normal.

- `show snmp-server statistics`
  
  This command shows the configured characteristics of the SNMP server. To reset all SNMP counters to zero, use the `clear snmp-server statistics` command.

- `show snmp-server user`
  
  This command shows the configured characteristics of users.

**Examples**

The following example shows how to display SNMP server statistics:

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
```
Examples for SNMP

0 Get-next PDUs
0 Get-bulk PDUs
0 Set-request PDUs (Not supported)
0 SNMP packets output
  0 Too big errors (Maximum packet size 512)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

The following example shows how to display the SNMP server running configuration:

ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

Examples for SNMP

This sections includes examples for all versions of SNMP.

SNMP Versions 1 and 2c

The following example shows how the ASA can receive SNMP requests from host 192.0.2.5 on the inside interface but does not send any SNMP syslog requests to any host:

ciscoasa(config)# snmp-server host 192.0.2.5

ciscoasa(config)# snmp-server location building 42

ciscoasa(config)# snmp-server contact EmployeeA

ciscoasa(config)# snmp-server community ohwhatakeyisthee

SNMP Version 3

The following example shows how the ASA can receive SNMP requests using the SNMP Version 3 security model, which requires that the configuration follow this specific order: group, followed by user, followed by host:

ciscoasa(config)# snmp-server group v3 vpn-group priv

ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123

ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
## History for SNMP

### Table 40-7 History for SNMP

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Versions 1 and 2c</td>
<td>7.0(1)</td>
<td>Provides ASA, ASAv, and ASASM network monitoring and event information by transmitting data between the SNMP server and SNMP agent through the clear text community string.</td>
</tr>
<tr>
<td>SNMP Version 3</td>
<td>8.2(1)</td>
<td>Provides 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 users, groups, and hosts, as well as authentication characteristics by using the USM. In addition, this version allows access control to the agent and MIB objects and includes additional MIB support. We introduced or modified the following commands: show snmp-server engineid, show snmp-server group, show snmp-server user, snmp-server group, snmp-server user, snmp-server host.</td>
</tr>
<tr>
<td>Password encryption</td>
<td>8.3(1)</td>
<td>Supports password encryption. We modified the following commands: snmp-server community, snmp-server host.</td>
</tr>
<tr>
<td>SNMP traps and MIBs</td>
<td>8.4(1)</td>
<td>Supports the following additional keywords: connection-limit-reached, cpu threshold rising, entity cpu-temperature, entity fan-failure, entity power-supply, ikev2 stop</td>
</tr>
<tr>
<td>IF-MIB ifAlias OID support</td>
<td>8.2(5)/8.4(2)</td>
<td>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.</td>
</tr>
</tbody>
</table>
The ASASM supports all MIBs and traps that are present in 8.4(1), except for the following:

Unsupported MIBs in 8.5(1):
- CISCO-ENTITY-SENSOR-EXT-MIB (Only objects under the entPhySensorTable group are supported).
- ENTITY-SENSOR-MIB (Only objects in the entPhySensorTable group are supported).
- DISMAN-EXPRESSION-MIB (Only objects in the expExpressionTable, expObjectTable, and expValueTable groups are supported).

Unsupported traps in 8.5(1):
- ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB). This trap is only used for power supply failure, fan failure, and high CPU temperature events.
- InterfacesBandwidthUtilization.

We modified the following command: `snmp-server enable traps`.

The following MIBs have been enabled for the ASASM:
- ALTIGA-GLOBAL-REG.my
- ALTIGA-LBSSF-STATS-MIB.my
- ALTIGA-MIB.my
- ALTIGA-SSL-STATS-MIB.my
- CISCO-IPSEC-FLOW-MONITOR-MIB.my
- CISCO-REMOTE-ACCESS-MONITOR-MIB.my

Support for the following MIB was added: CISCO-TRUSTSEC-SXP-MIB.

Five new SNMP Physical Vendor Type OIDs have been added to support the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.

Added the cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support the xlate_count and max_xlate_count entries, which are the equivalent to allowing polling using the `show xlate count` command.
### Table 40-7  History for SNMP (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP hosts, host groups, and user lists</td>
<td>9.1(5)</td>
<td>You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host. We introduced or modified the following commands: <code>snmp-server host-group</code>, <code>snmp-server user-list</code>, <code>show running-config snmp-server</code>, <code>clear configure snmp-server</code>.</td>
</tr>
<tr>
<td>SNMP message size</td>
<td>9.2(1)</td>
<td>The limit on the message size that SNMP sends has been increased to 1472 bytes.</td>
</tr>
<tr>
<td>SNMP OIDs and MIBs</td>
<td></td>
<td>The ASA now supports the <code>cpmCPUTotal5minRev OID</code>. The ASAv has been added as a new product to the SNMP sysObjectID OID and <code>entPhysicalVendorType OID</code>. The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the new ASAv platform. A new SNMP MIB for monitoring VPN shared license usage has been added.</td>
</tr>
<tr>
<td>SNMP OIDs and MIBs</td>
<td>9.3(1)</td>
<td>CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) support has been added for the ASASM.</td>
</tr>
</tbody>
</table>
| SNMP MIBs and traps           | 9.3(2)            | The CISCO-PRODUCTS-MIB and CISCO-ENTITY-VENDORTYPE-OID-MIB have been updated to support the ASA 5506-X. The ASA 5506-X has been added as new products to the SNMP sysObjectID OID and `entPhysicalVendorType OID` tables. The ASA now supports the CISCO-CONFIG-MAN-MIB, which enables you to do the following:  
  - Know which commands have been entered for a specific configuration.  
  - Notify the NMS when a change has occurred in the running configuration.  
  - Track the time stamps associated with the last time that the running configuration was changed or saved.  
  - Track other changes to commands, such as terminal details and command sources.  
  We modified the following command: `snmp-server enable traps`. |
Anonymous Reporting and Smart Call Home

This chapter describes how to configure the Anonymous Reporting and Smart Call Home services.

- About Anonymous Reporting, page 41-1
- About Smart Call Home, page 41-2
- Guidelines for Anonymous Reporting and Smart Call Home, page 41-7
- Configure Anonymous Reporting and Smart Call Home, page 41-8
- Monitoring Anonymous Reporting and Smart Call Home, page 41-18
- Examples for Smart Call Home, page 41-19
- History for Anonymous Reporting and Smart Call Home, page 41-20

About Anonymous Reporting

You can help to improve the Cisco ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device. If you enable the feature, your customer identity will remain anonymous, and no identifying information will be sent.

Enabling Anonymous Reporting creates a trust point and installs a certificate. A CA certificate is required for your ASA to validate the server certificate present on the Smart Call Home web server and to form the HTTPS session so that your ASA can send messages securely. Cisco imports a certificate that is predefined in the software. If you decide to enable Anonymous Reporting, a certificate is installed on the ASA with a hardcoded trust point name: _SmartCallHome_ServerCA. When you enable Anonymous Reporting, this trust point is created, the appropriate certificate is installed, and you receive a message about this action. The certificate then appears in your configuration.

If the appropriate certificate already exists in your configuration when you enable Anonymous Reporting, no trust point is created, and no certificate is installed.

Note

When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on Cisco’s behalf (including countries outside of the U.S.). Cisco maintains the privacy of all customers. For information about Cisco’s treatment of personal information, see the Cisco Privacy Statement at the following URL:
DNS Requirement

A DNS server must be configured correctly for the ASA to reach the Cisco Smart Call Home server and send messages to Cisco. Because it is possible that the ASA resides in a private network and does not have access to the public network, Cisco verifies your DNS configuration and then configures it for you, if necessary, by doing the following:

1. Performing a DNS lookup for all DNS servers configured.
2. Getting the DNS server from the DHCP server by sending DHCPINFORM messages on the highest security-level interface.
3. Using the Cisco DNS servers for lookup.

These tasks are performed without changing the current configuration. (For example, the DNS server that was learned from DHCP will not be added to the configuration.)

If there is no DNS server configured, and the ASA cannot reach the Cisco Smart Call Home Server, Cisco generates a syslog message with the warning severity level for each Smart Call Home message that is sent to remind you to configure DNS correctly.

See the syslog messages guide for information about syslog messages.

About Smart Call Home

When fully configured, Smart Call Home detects issues at your site and reports them back to Cisco or through other user-defined channels (such as e-mail or directly to you), often before you know that these issues exist. Depending on the seriousness of these problems, Cisco responds to your system configuration issues, product end-of-life announcements, security advisory issues, and so on by providing the following services:

- Identifying issues quickly with continuous monitoring, real-time proactive alerts, and detailed diagnostics.
- Making you aware of potential problems through Smart Call Home notifications, in which a service request has been opened, with all diagnostic data attached.
- Resolving critical problems faster with direct, automatic access to experts in Cisco TAC.
- Using staff resources more efficiently by reducing troubleshooting time.
- Generating service requests to Cisco TAC automatically (if you have a service contract), routed to the appropriate support team, which provides detailed diagnostic information that speeds problem resolution.

The Smart Call Home Portal offers quick access to required information that enables you to do the following:

- Review all Smart Call Home messages, diagnostics, and recommendations in one place.
- Check service request status.
- View the most up-to-date inventory and configuration information for all Smart Call Home-enabled devices.
Subscribe to Alert Groups

An alert group is a predefined subset of the Smart Call Home alerts that are supported on the ASA. Different types of Smart Call Home alerts are grouped into different alert groups, depending on their type. Each alert group reports the output of certain CLIs. The supported Smart Call Home alert groups are the following:

- syslog
- diagnostic
- environment
- inventory
- configuration
- threat
- snapshot
- telemetry
- test

Attributes of Alert Groups

Alert groups have the following attributes:

- Events first register with one alert group.
- A group can associate with multiple events.
- You can subscribe to specific alert groups.
- You can enable and disable specific alert groups. The default setting is enabled for all alert groups.
- The diagnostic and environment alert groups support subscription for periodic messages.
- The syslog alert group supports message ID-based subscription.
- You can configure a threshold for CPU and memory usage for the environment alert group. When a certain parameter has exceeded a predefined threshold, a message is sent. Most of the threshold values are platform-dependent and cannot be changed.
- You configure the snapshot alert group to send the output of CLIs that you specify.

Messages Sent to Cisco by Alert Groups

Messages are sent to Cisco periodically and whenever the ASA reloads. These messages are categorized by alert groups.

Inventory alerts consist of output from the following commands:

- **show version**—Displays the ASA software version, hardware configuration, license key, and related uptime data for the device.
- **show inventory**—Retrieves and displays inventory information about each Cisco product that is installed in the networking device. Each product is identified by unique device information, called the UDI, which is a combination of three separate data elements: the product identifier (PID), the version identifier (VID), and the serial number (SN).
Chapter 41  Anonymous Reporting and Smart Call Home

About Smart Call Home

- show failover state—Displays the failover state of both units in a failover pair. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and the last reported reason for failover.
- show module—Shows information about any modules installed on the ASAs, for example, information about an SSP installed on the ASA 5585-X, and information about an IPS SSP installed on an ASA 5585-X.
- show environment—Shows system environment information for ASA system components, such as hardware operational status for the chassis, drivers, fans, and power supplies, as well as temperature status, voltage, and CPU usage.

Configuration alerts consist of output from the following commands:

- show context—Shows allocated interfaces and the configuration file URL, the number of contexts configured, or if you enable Anonymous Reporting in the system execution space, from a list of all contexts.
- show call-home registered-module status—Shows the registered module status. If you use system configuration mode, the command displays system module status based on the entire device, not per context.
- show running-config—Shows the configuration that is currently running on the ASA.
- show startup-config—Show the startup configuration.
- show access-list | include elements—Shows the hit counters and a time stamp value for an access list.

Diagnostic alerts consist of output from the following commands:

- show failover—Displays information about the failover status of the unit.
- show interface—Displays interface statistics.
- show cluster info—Displays cluster information.
- show cluster history—Displays the cluster history.
- show crashinfo (truncated)—After an unexpected software reload, the device sends a modified crash information file with only the traceback section of the file included, so only function calls, register values, and stack dumps are reported to Cisco.
- show tech-support no-config—Displays the information that is used for diagnosis by technical support analysts.

Environment alerts consist of output from the following commands:

- show environment—Shows system environment information for ASA system components, such as hardware operational status for the chassis, drivers, fans, and power supplies, as well as temperature status, voltage, and CPU usage.
- show cpu usage—Displays CPU usage information.
- show memory detail—Displays details of the free and allocated system memory.

Threat alerts consist of output from the following commands:

- show threat-detection rate—Displays threat detection statistics.
- show threat-detection shun—Displays currently shunned hosts.
- show shun—Displays shun information.
- show dynamic-filter reports top—Generates reports of the top 10 malware sites, ports, and infected hosts classified by the Botnet Traffic Filter.
Snapshot alerts may consist of output from the following commands:

- `show conn count`—Shows the number of active connections.
- `show asp drop`—Shows the accelerated security path dropped packets or connections.

Telemetry alerts consist of output from the following commands:

- `show perfmon detail`—Shows ASA performance details.
- `show traffic`—Displays interface transmit and receive activity.
- `show conn count`—Shows the number of active connections.
- `show vpn-sessiondb summary`—Shows VPN session summary information.
- `show vpn load-balancing`—Displays the runtime statistics for the VPN load-balancing virtual cluster configuration.
- `show local-host | include interface`—Shows the network states of local hosts.
- `show memory`—Displays a summary of the maximum physical memory and current free memory available to the operating system.
- `show context`—Shows allocated interfaces and the configuration file URL, the number of contexts configured, or if you enable Anonymous Reporting in the system execution space, from a list of all contexts.
- `show access-list | include elements`—Shows the hit counters and a time stamp value for an access list.
- `show interface`—Displays interface statistics.
- `show threat-detection statistics protocol`—Shows IP protocol statistics.
- `show phone-proxy media-sessions count`—Displays the number of corresponding media sessions stored by the Phone Proxy.
- `show phone-proxy secure-phones count`—Displays the number of phones capable of secure mode stored in the database.
- `show route`—Displays the routing table.
- `show xlate count`—Shows the number of NAT sessions (xlates).

**Message Severity Threshold**

When you subscribe a destination profile to certain alert groups, you can set a threshold for sending alert group messages based on the message severity level. Any message with a value lower than the destination profile’s specified threshold is not sent to the destination.

Table 41-1 shows the mapping between message severity levels and syslog severity levels.

<table>
<thead>
<tr>
<th>Level</th>
<th>Message Severity Level</th>
<th>Syslog Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Catastrophic</td>
<td>N/A</td>
<td>Network-wide catastrophic failure.</td>
</tr>
<tr>
<td>8</td>
<td>Disaster</td>
<td>N/A</td>
<td>Significant network impact.</td>
</tr>
</tbody>
</table>
Table 41-1  Message Severity Level and Syslog Level Mapping (continued)

<table>
<thead>
<tr>
<th>Level</th>
<th>Message Severity Level</th>
<th>Syslog Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Determined by the specified CLI keyword: <code>subscribe-to-alert-group name of alert group severity severity level</code></td>
<td>0</td>
<td>Emergency. System is unusable.</td>
</tr>
<tr>
<td>6</td>
<td>Determined by the specified CLI keyword: <code>subscribe-to-alert-group name of alert group severity severity level</code></td>
<td>1</td>
<td>Alert. Critical conditions; immediate attention needed.</td>
</tr>
<tr>
<td>5</td>
<td>Determined by the specified CLI keyword: <code>subscribe-to-alert-group name of alert group severity severity level</code></td>
<td>2</td>
<td>Critical. Major conditions.</td>
</tr>
<tr>
<td>4</td>
<td>Determined by the specified CLI keyword: <code>subscribe-to-alert-group name of alert group severity severity level</code></td>
<td>3</td>
<td>Error. Minor conditions.</td>
</tr>
<tr>
<td>3</td>
<td>Warning</td>
<td>4</td>
<td>Warning conditions.</td>
</tr>
<tr>
<td>2</td>
<td>Notification</td>
<td>5</td>
<td>Basic notification and informational messages. Possibly independently insignificant.</td>
</tr>
<tr>
<td>1</td>
<td>Normal</td>
<td>6</td>
<td>Information. Normal event, signifying a return to normal state.</td>
</tr>
<tr>
<td>0</td>
<td>Debugging</td>
<td>7</td>
<td>Debugging messages (default setting).</td>
</tr>
</tbody>
</table>

Subscription Profiles

A subscription profile allows you to associate the destination recipients with interested groups. When an event registered with a subscribed group in a profile is triggered, the message associated with the event is sent to the configured recipients. Subscription profiles have the following attributes:

- You can create and configure multiple profiles.
- A profile may configure multiple e-mail or HTTPS recipients.
- A profile may subscribe multiple groups to a specified severity level.
A profile supports three message formats: short text, long text, and XML.
You can enable and disable a specific profile. Profiles are disabled by default.
You can specify the maximum message size. The default is 3 MB.

A default profile, “Cisco TAC,” has been provided. The default profile has a predefined set of groups (diagnostic, environment, inventory, configuration, and telemetry) to monitor and predefined destination e-mail and HTTPS URLs. The default profile is created automatically when you initially configure Smart Call Home. The destination e-mail is callhome@cisco.com and the destination URL is https://tools.cisco.com/its/service/oddce/services/DDCEService.

Note
You cannot change the destination e-mail or the destination URL of the default profile.

When you subscribe a destination profile to the configuration, inventory, telemetry, or snapshot alert groups, you can choose to receive the alert group messages asynchronously or periodically at a specified time.

Table 41-2 maps the default alert group to its severity level subscription and period (if applicable):

**Table 41-2  Alert Group to Severity Level Subscription Mapping**

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Severity Level</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Informational</td>
<td>Monthly</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Informational and higher</td>
<td>N/A</td>
</tr>
<tr>
<td>Environment</td>
<td>Notification and higher</td>
<td>N/A</td>
</tr>
<tr>
<td>Inventory</td>
<td>Informational</td>
<td>Monthly</td>
</tr>
<tr>
<td>Snapshot</td>
<td>Informational</td>
<td>N/A</td>
</tr>
<tr>
<td>Syslog</td>
<td>Equivalent syslog</td>
<td>N/A</td>
</tr>
<tr>
<td>Telemetry</td>
<td>Informational</td>
<td>Daily</td>
</tr>
<tr>
<td>Test</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Threat</td>
<td>Notification</td>
<td>N/A</td>
</tr>
</tbody>
</table>

## Guidelines for Anonymous Reporting and Smart Call Home

This section includes the guidelines and limitations that you should check before configuring Anonymous Reporting and Smart Call Home.

**Anonymous Reporting Guidelines**
- DNS must be configured.
- If an Anonymous Reporting message cannot be sent on the first try, the ASA retries two more times before dropping the message.
- Anonymous Reporting may coexist with other Smart Call Home configurations without changing the existing configuration. For example, if Smart Call Home is disabled before enabling Anonymous Reporting, it remains disabled, even after Anonymous Reporting has been enabled.
- If Anonymous Reporting is enabled, you cannot remove the trust point, and when Anonymous Reporting is disabled, the trust point remains. If Anonymous Reporting is disabled, you can remove the trust point, but disabling Anonymous Reporting does not cause the trust point to be removed.
If you are using a multiple context mode configuration, the `dns`, `interface`, and `trustpoint` commands are in the admin context, and the `call-home` commands are in the system context.

**Smart Call Home Guidelines**

- In multiple context mode, the `subscribe-to-alert-group snapshot periodic` command is divided into two commands: one to obtain information from the system configuration and one to obtain information from the user context.
- The Smart Call Home back-end server can accept messages in XML format only.
- A Smart Call Home message is sent to Cisco to report important cluster events if you have enabled clustering and configured Smart Call Home to subscribe to the diagnostic alert group with a critical severity level. A Smart Call Home clustering message is sent for only the following events:
  - When a unit joins the cluster
  - When a unit leaves the cluster
  - When a cluster unit becomes the cluster master
  - When a secondary unit fails in the cluster
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

**Related Topics**

- DNS Requirement, page 41-2
- Configure the DNS Server, page 14-14

**Configure Anonymous Reporting and Smart Call Home**

While Anonymous Reporting is part of the Smart Call Home service and allows Cisco to anonymously receive minimal error and health information from your device, the Smart Call Home service provides customized support of your system health, enabling Cisco TAC to monitor your devices and open a case when there is an issue, often before you know the issue has occurred.

You can have both services configured on your system at the same time, although configuring the Smart Call Home service provides the same functionality as Anonymous Reporting, plus customized services.

When you enter configuration mode, you receive a prompt that requests you to enable the Anonymous Reporting and Smart Call Home services according to the following guidelines:

- At the prompt, you may choose [Y]es, [N]o, [A]sk later. If you choose [A]sk later, then you are reminded again in seven days or when the ASA reloads. If you continue to choose [A]sk later, the ASA prompts two more times at seven-day intervals before it assumes a [N]o response and does not ask again.
- If you did not receive the prompt, you may enable Anonymous Reporting or Smart Call Home by performing the steps in Configure Anonymous Reporting, page 41-9 or in Configure Smart Call Home, page 41-9.
Configure Anonymous Reporting

To configure Anonymous Reporting, perform the following steps:

**Procedure**

**Step 1**  Enable the Anonymous Reporting feature and create a new anonymous profile.
```
call-home reporting anonymous
```
Example:
```
ciscoasa(config)# call-home reporting anonymous
```
Entering this command creates a trust point and installs a certificate that is used to verify the identity of the Cisco web server.

**Step 2**  (Optional) Make sure that you have connectivity to the server and that your system can send messages.
```
call-home test reporting anonymous
```
Example:
```
ciscoasa(config)# call-home test reporting anonymous
INFO: Sending test message to https://tools.cisco.com/its/service/oddce/services/DDCEService... 
INFO: Succeeded
```
A success or error message returns test results.

Configure Smart Call Home

Configuring the Smart Call Home service on your ASA includes the following tasks:

**Step 1**  Enable the Smart Call Home service. See Enable Smart Call Home, page 41-10.

**Step 2**  Configure the mail server through which Smart Call Home messages are delivered to subscribers. See Configure the Mail Server, page 41-14.

**Step 3**  Set up contact information for the Smart Call Home messages. See Configure Customer Contact Information, page 41-13.

**Step 4**  Define alert processing parameters, such as the maximum rate of events that can be handled. See Configure Alert Group Subscription, page 41-12.

**Step 5**  Set up alert subscription profiles. See Configure a Destination Profile, page 41-16.

Each alert subscription profile identifies the following:

- The subscribers to whom the Smart Call Home messages are sent, such as a Smart Call Home server at Cisco or a list of e-mail recipients.
- Information categories for which you want to receive alerts, such as configuration or inventory information.
Enable Smart Call Home

To enable Smart Call Home and activate your call-home profile, perform the following steps:

Procedure

Step 1  Enable the Smart Call Home service.

```
service call-home
```

Example:
```
ciscoasa(config)# service call-home
```

Step 2  Enter call-home configuration mode.

```
call-home
```

Example:
```
ciscoasa(config)# call home
```

Declare and Authenticate a Certificate Authority Trust Point

If Smart Call Home is configured to send messages to a web server through HTTPS, you need to configure the ASA to trust the certificate of the web server or the certificate of the Certificate Authority (CA) that issued the certificate. The Cisco Smart Call Home Production server certificate is issued by Verisign. The Cisco Smart Call Home Staging server certificate is issued by the Digital Signature Trust Company.

**Note**
You should set the trust point for no client-types/no validation-usage to prevent it from being used for VPN validation.

To declare and authenticate the Cisco server security certificate and establish communication with the Cisco HTTPS server for Smart Call Home service, perform the following steps:

Procedure

Step 1  (Multiple Context Mode only) Install the certificate in the admin context.

```
changeto context admin-context
```

Example:
```
ciscoasa(config)# changeto context contextA
```

Step 2  Configure a trust point and prepare for certificate enrollment.

```
crypto ca trustpoint trustpoint-name
```
Example:

ciscoasa(config)# crypto ca trustpoint cisco

**Note** If you use HTTP as the transport method, you must install a security certificate through a trust point, which is required for HTTPS. Find the specific certificate to install at the following URL:


---

**Step 3** Specify a manual cut-and-paste method of certificate enrollment.

`enroll terminal`

Example:

ciscoasa(ca-trustpoint)# enroll terminal

**Step 4** Authenticate the named CA. The CA name should match the trust point name specified in the `crypto ca trustpoint` command. At the prompt, paste the security certificate text.

`crypto ca authenticate trustpoint`

Example:

ciscoasa(ca-trustpoint)# crypto ca authenticate cisco

**Step 5** Specify the end of the security certificate text and confirm acceptance of the entered security certificate.

`quit`

Example:

ciscoasa(ca-trustpoint)# quit

%Do you accept this certificate [yes/no]:

`yes`

---

**Configure the Environment and Snapshot Alert Groups**

To configure the environment and snapshot alert groups, perform the following steps:

**Procedure**

**Step 1** Enter alert-group-configuration mode.

`alert-group-config (environment | snapshot)`

Example:

ciscoasa(config)# alert-group-config environment
Configure Alert Group Subscription

To subscribe a destination profile to an alert group, perform the following steps:

Procedure

**Step 1** Enter call-home configuration mode.
```
call-home
```
Example:
```
ciscoasa(config)# call-home
```

**Step 2** Enable the specified Smart Call Home alert group.
```
alert-group {all | configuration | diagnostic | environment | inventory | syslog}
```
Example:
```
ciscoasa(cfg-call-home)# alert-group syslog
```
Use the **all** keyword to enable all alert groups. By default, all alert groups are enabled.

**Step 3** Enter the profile configuration mode for the specified destination profile.
```
profile profile-name
```
Example:
```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

**Step 4** Subscribe to all available alert groups.
```
subscribe-to-alert-group all
```
Example:
```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

**Step 5** Subscribe this destination profile to the configuration alert group.
```
subscribe-to-alert-group configuration periodic {daily hh:mm | monthly date hh:mm | weekly day hh:mm}
```
Example:
```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly Wednesday 23:30
```

The **periodic** keyword configures the configuration alert group for periodic notification. The default period is daily.

The **daily** keyword specifies the time of the day to send, in the **hh:mm** format, with a 24-hour clock (for example, 14:30).

The **weekly** keyword specifies the day of the week and time of day in the **day hh:mm** format, where the day of the week is spelled out (for example, Monday).

The **monthly** keyword specifies the numeric date, from 1 to 31, and the time of day, in the **date hh:mm** format.
Configure Customer Contact Information

To configure customer contact information, perform the following steps:

Procedure

Step 1  Enter call-home configuration mode.

`call-home`

Example:
`ciscoasa(config)# call-home`

Step 2  Specify the customer phone number. Spaces are allowed, but you must use quotes around the string if it includes spaces.

`phone-number phone-number-string`

Example:
`ciscoasa(cfg-call-home)# phone-number 8005551122`

Step 3  Specify the customer address, which is a free-format string that may be up to 255 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

`street-address street-address`

Example:
`ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"`

Step 4  Specify the customer name, which may be up to 128 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

`contact-name contact-name`

Example:
`ciscoasa(cfg-call-home)# contact-name contactname1234`

Step 5  Specify the Cisco customer ID, which may be up to 64 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

`customer-id customer-id-string`

Example:
`ciscoasa(cfg-call-home)# customer-id customer1234`

Step 6  Specify the customer site ID, which may be up to 64 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

`site-id site-id-string`

Example:
`ciscoasa(cfg-call-home)# site-id site1234`

Step 7  Specify the customer contract identification, which may be up to 128 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

`contract-id contract-id-string`
Example:
ciscoasa(cfg-call-home)# contract-id contract1234

Examples
The following example shows how to configure contact information:
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234

Configure the Mail Server

We recommend that you use HTTPS for message transport because it is the most secure. However, you may configure an e-mail destination for Smart Call Home and then configure the mail server to use the e-mail message transport.

To configure the mail server, perform the following steps:

Procedure

Step 1
Enter call-home configuration mode.

call-home

Example:
ciscoasa(config)# call-home

Step 2
Specify the SMTP mail server.

mail-server ip-address name priority [1-100] [all]

Example:
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1

You can specify up to five mail servers, using five separate commands. You must configure at least one mail server for using e-mail transport of Smart Call Home messages.
The lower the number, the higher the priority of the mail server.
The ip-address argument can be an IPv4 or IPv6 mail server address.

Examples
The following example shows how to configure a primary mail server (named”smtp.example.com”) and a secondary mail server at IP address 10.10.1.1:
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
Configure Traffic Rate Limiting

To configure traffic rate limiting, perform the following steps:

**Procedure**

**Step 1** Enter call-home configuration mode.

`call-home`

Example:

```
ciscoasa(config)# call-home
```

**Step 2** Specify the number of messages that Smart Call Home can send per minute. The default value is 10 messages per minute.

`rate-limit msg-count`

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Send Smart Call Home Communications

To send a Smart Call Home test message manually, perform the following steps:

**Procedure**

**Step 1** Send a test message using a profile configuration.

`call-home test [test-message] profile profile-name`

Example:

```
ciscoasa# call-home test [testing123] profile CiscoTAC-1
```

To trigger an alert group message manually, perform the following steps:

**Procedure**

**Step 1** Send an alert group message to one destination profile, if specified. If no profile is specified, send messages to all profiles that are subscribed to the inventory, configuration, snapshot, or telemetry alert groups.

`call-home send alert-group {inventory | configuration | snapshot | telemetry} [profile profile-name]`

Example:
Configure Anonymous Reporting and Smart Call Home

To issue a CLI command and e-mail the command output to Cisco TAC or to an e-mail address that you specify, perform the following steps:

**Procedure**

**Step 1** Send command output to an e-mail address. The specified CLI command can be any command, including commands for all registered modules.

```
call-home send cli command [email email]
```

Example:

```
ciscoasa# call-home send cli destination email username@example.com
```

If you specify an e-mail address, the command output is sent to that address. If no e-mail address is specified, the output is sent to Cisco TAC. The e-mail is sent in log text format with the service number, if specified, in the subject line.

The service number is required only if no e-mail address is specified, or if a Cisco TAC e-mail address is specified.

**Configure a Destination Profile**

To configure a destination profile for e-mail or for HTTP, perform the following steps:

**Procedure**

**Step 1** Enter call-home configuration mode.

```
call-home
```

Example:

```
ciscoasa(config)# call-home
```

**Step 2** Enter the profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.

```
profile profile-name
```

Example:

```
ciscoasa(cfg-call-home)# profile newprofile
```

You can create a maximum of 10 active profiles. The default profile is to report back to Cisco TAC. If you want to send call home information to a different location (for example, your own server), you can configure a separate profile.

**Step 3** Configure the destination, message size, message format, and transport method for the Smart Call Home message receiver. The default message format is XML, and the default enabled transport method is e-mail.
Configure Anonymous Reporting and Smart Call Home

destination {email address | http url} | message-size-limit size | preferred-msg-format {long-text | short-text | xml} transport-method {email | http}}

Example:
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text

The e-mail-address is the e-mail address of the Smart Call Home message receiver, which can be up to 100 characters long. By default, the maximum URL size is 5 MB.

Use the short-text format to send and read a message on a mobile device, and use the long text format to send and read a message on a computer.

If the message receiver is the Smart Call Home back-end server, ensure that the preferred-msg-format value is XML because the back-end server can accept messages in XML format only.

See Enable Smart Call Home, page 41-10 to set the transport method to HTTP. Use this command to change the transport method back to e-mail.

---

Copy a Destination Profile

To create a new destination profile by copying an existing one, perform the following steps:

**Procedure**

**Step 1** Enter call-home configuration mode.
call-home

Example:
ciscoasa(config)# call-home

**Step 2** Specify the profile to copy.
profile profile-name

Example:
ciscoasa(cfg-call-home)# profile newprofile

**Step 3** Copy the content of an existing profile to a new profile.
copy profile src-profile-name dest-profile-name

Example:
ciscoasa(cfg-call-home)# copy profile newprofile profile1

The existing profile (src-profile-name) and the new profile (dest-profile-name) may be up to 23 characters long.

**Examples**
The following example shows how to copy an existing profile:
ciscoasa(config)# call-home
Ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1

Rename a Destination Profile

To change the name of an existing profile, perform the following steps:

Procedure

**Step 1** Enter call-home configuration mode.

```
call-home
```

Example:
```
ciscoasa(config)# call-home
```

**Step 2** Specify the profile to rename.

```
profile profilename
```

Example:
```
ciscoasa(cfg-call-home)# profile newprofile
```

**Step 3** Change the name of an existing profile.

```
rename profile src-profile-name dest-profile-name
```

Example:
```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

The existing profile (*src-profile-name*) and the new profile (*dest-profile-name*) may be up to 23 characters long.

**Examples**

The following example shows how to rename an existing profile:
```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

Monitoring Anonymous Reporting and Smart Call Home

See the following commands for monitoring Anonymous Reporting and Smart Call Home services:

- **show call-home detail**
  
  This command shows the current Smart Call Home detail configuration.

- **show call-home mail-server status**
  
  This command shows the current mail server status.

- **show call-home profile {profile name | all}**
This command shows the configuration of Smart Call Home profiles.

- **show call-home registered-module status [all]**
  This command shows the registered module status.

- **show call-home statistics**
  This command shows call-home detail status.

- **show call-home**
  This command shows the current Smart Call Home configuration.

- **show running-config call-home**
  This command shows the current Smart Call Home running configuration.

- **show smart-call-home alert-group**
  This command shows the current status of Smart Call Home alert groups.

- **show running-config all**
  This command shows details about the Anonymous Reporting user profile.

---

**Examples for Smart Call Home**

The following example shows how to configure the Smart Call Home service:

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30

ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly Wednesday 23:30

ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment

ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic

```

Monday 23:30
## History for Anonymous Reporting and Smart Call Home

### Table 41-3  History for Anonymous Reporting and Smart Call Home

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Call Home</td>
<td>8.2(2)</td>
<td>The Smart Call Home service offers proactive diagnostics and real-time alerts on the ASA, and provides higher network availability and increased operational efficiency. We introduced or modified the following commands: active (call home), call-home, call-home send alert-group, call-home test, contact-email-addr, customer-id (call home), destination (call home), profile, rename profile, service call-home, show call-home, show call-home detail, show smart-call-home alert-group, show call-home profile, show call-home statistics, show call-home mail-server status, show running-config call-home, show call-home registered-module status all, site-id, street-address, subscribe-to-alert-group all, alert-group-config, subscribe-to-alert-group configuration, subscribe-to-alert-group diagnostic, subscribe-to-alert-group environment, subscribe-to-alert-group inventory periodic, subscribe-to-alert-group snapshot periodic, subscribe-to-alert-group syslog, subscribe-to-alert-group telemetry periodic.</td>
</tr>
<tr>
<td>Anonymous Reporting</td>
<td>9.0(1)</td>
<td>You can help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from a device. We introduced the following commands: call-home reporting anonymous, call-home test reporting anonymous.</td>
</tr>
</tbody>
</table>
Smart Call Home 9.1(2) The `show local-host` command was changed to the `show local-host | include interface` command for telemetry alert group reporting.

Smart Call Home 9.1(3) A Smart Call Home message is sent to Cisco to report important cluster events if you have enabled clustering and configured Smart Call Home to subscribe to the Diagnostic alert group with a Critical severity level. 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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Call Home</td>
<td>9.1(2)</td>
<td>The <code>show local-host</code> command was changed to the `show local-host</td>
</tr>
</tbody>
</table>
| Smart Call Home | 9.1(3) | A Smart Call Home message is sent to Cisco to report important cluster events if you have enabled clustering and configured Smart Call Home to subscribe to the Diagnostic alert group with a Critical severity level. 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 |
PART 10

Reference
This chapter describes how to use the CLI on the Cisco ASA.

- Firewall Mode and Security Context Mode, page 42-1
- Command Modes and Prompts, page 42-2
- Syntax Formatting, page 42-3
- Abbreviate Commands, page 42-3
- Command-Line Editing, page 42-3
- Command Completion, page 42-4
- Command Help, page 42-4
- View the Running Configuration, page 42-4
- Filter show and more Command Output, page 42-5
- Command Output Paging, page 42-5
- Add Comments, page 42-6
- Text Configuration Files, page 42-6
- Supported Character Sets, page 42-8

Note

The CLI uses similar syntax and other conventions to the Cisco IOS CLI, but the ASA operating system is not a version of Cisco IOS software. Do not assume that a Cisco IOS CLI command works with or has the same function on the ASA.

Firewall Mode and Security Context Mode

The ASA runs in a combination of the following modes:

- Transparent firewall or routed firewall mode
  
  The firewall mode determines if the ASA runs as a Layer 2 or Layer 3 firewall.

- Multiple context or single context mode
  
  The security context mode determines if the ASA runs as a single device or as multiple security contexts, which act like virtual devices.

Some commands are only available in certain modes.
Command Modes and Prompts

The ASA CLI includes command modes. Some commands can only be entered in certain modes. For example, to enter commands that show sensitive information, you need to enter a password and enter a more privileged mode. Then, to ensure that configuration changes are not entered accidentally, you have to enter a configuration mode. All lower commands can be entered in higher modes, for example, you can enter a privileged EXEC command in global configuration mode.

Note

The various types of prompts are all default prompts and when configured, they can be different.

- When you are in the system configuration or in single context mode, the prompt begins with the hostname:
  ciscoasa

- When printing the prompt string, the prompt configuration is parsed and the configured keyword values are printed in the order in which you have set the `prompt` command. The keyword arguments can be any of the following and in any order: hostname, domain, context, priority, state.

  `asa(config)# prompt hostname context priority state`

- When you are within a context, the prompt begins with the hostname followed by the context name:
  ciscoasa/context

The prompt changes depending on the access mode:

- User EXEC mode
  User EXEC mode lets you see minimum ASA settings. The user EXEC mode prompt appears as follows when you first access the ASA:
  ciscoasa>
  ciscoasa/context>

- Privileged EXEC mode
  Privileged EXEC mode lets you see all current settings up to your privilege level. Any user EXEC mode command will work in privileged EXEC mode. Enter the `enable` command in user EXEC mode, which requires a password, to start privileged EXEC mode. The prompt includes the number sign (#):
  ciscoasa#
  ciscoasa/context#

- Global configuration mode
  Global configuration mode lets you change the ASA configuration. All user EXEC, privileged EXEC, and global configuration commands are available in this mode. Enter the `configure terminal` command in privileged EXEC mode to start global configuration mode. The prompt changes to the following:
  ciscoasa(config)#
  ciscoasa/context(config)#

- Command-specific configuration modes
From global configuration mode, some commands enter a command-specific configuration mode. All user EXEC, privileged EXEC, global configuration, and command-specific configuration commands are available in this mode. For example, the **interface** command enters interface configuration mode. The prompt changes to the following:

```
ciscoasa(config-if)#

ciscoasa/context(config-if)#
```

### Syntax Formatting

Command syntax descriptions use the conventions listed in Table 42-1.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>italics</em></td>
<td>Italic text indicates arguments for which you supply values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td></td>
<td>A vertical bar indicates a choice within an optional or required set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
</tbody>
</table>

### Abbreviate Commands

You can abbreviate most commands down to the fewest unique characters for a command; for example, you can enter `wr t` to view the configuration instead of entering the full command `write terminal`, or you can enter `en` to start privileged mode and `conf t` to start configuration mode. In addition, you can enter `0` to represent `0.0.0.0`.

### Command-Line Editing

The ASA uses the same command-line editing conventions as Cisco IOS software. You can view all previously entered commands with the `show history` command or individually with the up arrow or `^p` command. Once you have examined a previously entered command, you can move forward in the list with the down arrow or `^n` command. When you reach a command you wish to reuse, you can edit it or press the `Enter` key to start it. You can also delete the word to the left of the cursor with `^w`, or erase the line with `^u`.

The ASA permits up to 512 characters in a command; additional characters are ignored.
Command Completion

To complete a command or keyword after entering a partial string, press the Tab key. The ASA only completes the command or keyword if the partial string matches only one command or keyword. For example, if you enter s and press the Tab key, the ASA does not complete the command because it matches more than one command. However, if you enter dis, the Tab key completes the disable command.

Command Help

Help information is available from the command line by entering the following commands:

- `help command_name`
  Shows help for the specific command.
- `command_name ?`
  Shows a list of arguments available.
- `string? (no space)`
  Lists the possible commands that start with the string.
- `? and +?`
  Lists all commands available. If you enter ?, the ASA shows only commands available for the current mode. To show all commands available, including those for lower modes, enter +?.

Note

If you want to include a question mark (?) in a command string, you must press Ctrl-V before typing the question mark so that you do not inadvertently invoke CLI help.

View the Running Configuration

To view the running configuration, use one of the following commands:

- `show running-config [all] [command]`
  If you specify all, then all default settings are shown as well. If you specify a command, then the output only includes related commands.

  Note
  Many passwords are shown as *****. To view the passwords in plain text, or in encrypted form if you have a master passphrase enabled, use the more command.

- `more system:running-config`

Related Topics

Configure the Master Passphrase, page 14-10
Filter show and more Command Output

You can use the vertical bar (|) with any show command and include a filter option and filtering expression. The filtering is performed by matching each output line with a regular expression, similar to Cisco IOS software. By selecting different filter options you can include or exclude all output that matches the expression. You can also display all output beginning with the line that matches the expression.

The syntax for using filtering options with the show command is as follows:

```plaintext
ciscoasa# show command | {include | exclude | begin | grep [-v]} regexp
```

or

```plaintext
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

**Note**

Entering the more command allows you to view the contents of any file, not just the running configuration; see the command reference for more information.

In this command string, the first vertical bar (|) is the operator and must be included in the command. This operator directs the output of the show command to the filter. In the syntax diagram, the other vertical bars (|) indicate alternative options and are not part of the command.

The **include** option includes all output lines that match the regular expression. The **grep** option without -v has the same effect. The **exclude** option excludes all output lines that match the regular expression. The **grep** option with -v has the same effect. The **begin** option shows all the output lines starting with the line that matches the regular expression.

Replace **regexp** with any Cisco IOS regular expression. The regular expression is not enclosed in quotes or double-quotes, so be careful with trailing white spaces, which will be taken as part of the regular expression.

When creating regular expressions, you can use any letter or number that you want to match. In addition, certain keyboard characters called *metacharacters* have special meaning when used in regular expressions.

Use **Ctrl+V** to escape all of the special characters in the CLI, such as a question mark (?) or a tab. For example, type `d[Ctrl+V]?g` to enter `d?g` in the configuration.

Command Output Paging

For commands such as **help** or ?, **show**, **show xlate**, or other commands that provide long listings, you can determine if the information displays a screen and pauses, or lets the command run to completion. The **pager** command lets you choose the number of lines to display before the More prompt appears.

When paging is enabled, the following prompt appears:

```
<--- More --->
```

The More prompt uses syntax similar to the UNIX **more** command:

- Press the **Space** bar to view another screen.
- Press the **Enter** key to view the next line.
- Press the **q** key to return to the command line.
Add Comments

You can precede a line with a colon (:) to create a comment. However, the comment only appears in the command history buffer and not in the configuration. Therefore, you can view the comment with the show history command or by pressing an arrow key to retrieve a previous command, but because the comment is not in the configuration, the write terminal command does not display it.

Text Configuration Files

This section describes how to format a text configuration file that you can download to the ASA.

- How Commands Correspond with Lines in the Text File, page 42-6
- Command-Specific Configuration Mode Commands, page 42-6
- Automatic Text Entries, page 42-7
- Line Order, page 42-7
- Commands Not Included in the Text Configuration, page 42-7
- Passwords, page 42-7
- Multiple Security Context Files, page 42-7

How Commands Correspond with Lines in the Text File

The text configuration file includes lines that correspond with the commands described in this guide. In examples, commands are preceded by a CLI prompt. The prompt in the following example is “ciscoasa(config)#”:

```
ciscoasa(config)# context a
```

In the text configuration file you are not prompted to enter commands, so the prompt is omitted:

```
context a
```

Command-Specific Configuration Mode Commands

Command-specific configuration mode commands appear indented under the main command when entered at the command line. Your text file lines do not need to be indented, as long as the commands appear directly following the main command. For example, the following unindented text is read the same as indented text:

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
  nameif outside
```
Automatic Text Entries

When you download a configuration to the ASA, it inserts some lines automatically. For example, the ASA inserts lines for default settings or for the time the configuration was modified. You do not need to enter these automatic entries when you create your text file.

Line Order

For the most part, commands can be in any order in the file. However, some lines, such as ACEs, are processed in the order they appear, and the order can affect the function of the access list. Other commands might also have order requirements. For example, you must enter the nameif command for an interface first because many subsequent commands use the name of the interface. Also, commands in a command-specific configuration mode must directly follow the main command.

Commands Not Included in the Text Configuration

Some commands do not insert lines in the configuration. For example, a runtime command such as show running-config does not have a corresponding line in the text file.

Passwords

The login, enable, and user passwords are automatically encrypted before they are stored in the configuration. For example, the encrypted form of the password “cisco” might look like jMorNbk0514fadBh. You can copy the configuration passwords to another ASA in its encrypted form, but you cannot unencrypt the passwords yourself.

If you enter an unencrypted password in a text file, the ASA does not automatically encrypt it when you copy the configuration to the ASA. The ASA only encrypts it when you save the running configuration from the command line using the copy running-config startup-config or write memory command.

Multiple Security Context Files

For multiple security contexts, the entire configuration consists of the following multiple parts:

- The security context configurations
- The system configuration, which identifies basic settings for the ASA, including a list of contexts
- The admin context, which provides network interfaces for the system configuration

The system configuration does not include any 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 a context that is designated as the admin context.

Each context is similar to a single context mode configuration. The system configuration differs from a context configuration in that the system configuration includes system-only commands (such as a list of all contexts) while other typical commands are not present (such as many interface parameters).
Supported Character Sets

The ASA CLI currently supports UTF-8 encoding only. UTF-8 is the particular encoding scheme for Unicode symbols, and has been designed to be compatible with an ASCII subset of symbols. ASCII characters are represented in UTF-8 as one-byte characters. All other characters are represented in UTF-8 as multibyte symbols.

The ASCII printable characters (0x20 to 0x7e) are fully supported. The printable ASCII characters are the same as ISO 8859-1. UTF-8 is a superset of ISO 8859-1, so the first 256 characters (0-255) are the same as ISO 8859-1. The ASA CLI supports up to 255 characters (multibyte characters) of ISO 8859-1.
Addresses, Protocols, and Ports

This chapter provides a quick reference for IP addresses, protocols, and applications.

- IPv4 Addresses and Subnet Masks, page 43-1
- IPv6 Addresses, page 43-5
- Protocols and Applications, page 43-10
- TCP and UDP Ports, page 43-11
- Local Ports and Protocols, page 43-14
- ICMP Types, page 43-15

IPv4 Addresses and Subnet Masks

This section describes how to use IPv4 addresses in the Cisco ASA. An IPv4 address is a 32-bit number written in dotted-decimal notation: four 8-bit fields (octets) converted from binary to decimal numbers, separated by dots. The first part of an IP address identifies the network on which the host resides, while the second part identifies the particular host on the given network. The network number field is called the network prefix. All hosts on a given network share the same network prefix but must have a unique host number. In classful IP, the class of the address determines the boundary between the network prefix and the host number.

Classes

IP host addresses are divided into three different address classes: Class A, Class B, and Class C. Each class fixes the boundary between the network prefix and the host number at a different point within the 32-bit address. Class D addresses are reserved for multicast IP.

- Class A addresses (1.xxx.xxx.xxx through 126.xxx.xxx.xxx) use only the first octet as the network prefix.
- Class B addresses (128.0.xxx.xxx through 191.255.xxx.xxx) use the first two octets as the network prefix.
- Class C addresses (192.0.0.xxx through 223.255.255.xxx) use the first three octets as the network prefix.

Because Class A addresses have 16,777,214 host addresses, and Class B addresses 65,534 hosts, you can use subnet masking to break these huge networks into smaller subnets.
Private Networks

If you need large numbers of addresses on your network, and they do not need to be routed on the Internet, you can use private IP addresses that the Internet Assigned Numbers Authority (IANA) recommends (see RFC 1918). The following address ranges are designated as private networks that should not be advertised:

- 10.0.0.0 through 10.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

Subnet Masks

A subnet mask lets you convert a single Class A, B, or C network into multiple networks. With a subnet mask, you can create an extended network prefix that adds bits from the host number to the network prefix. For example, a Class C network prefix always consists of the first three octets of the IP address. But a Class C extended network prefix uses part of the fourth octet as well.

Subnet masking is easy to understand if you use binary notation instead of dotted decimal. The bits in the subnet mask have a one-to-one correspondence with the Internet address:

- The bits are set to 1 if the corresponding bit in the IP address is part of the extended network prefix.
- The bits are set to 0 if the bit is part of the host number.

**Example 1:** If you have the Class B address 129.10.0.0 and you want to use the entire third octet as part of the extended network prefix instead of the host number, then you must specify a subnet mask of 11111111.11111111.11111111.00000000. This subnet mask converts the Class B address into the equivalent of a Class C address, where the host number consists of the last octet only.

**Example 2:** If you want to use only part of the third octet for the extended network prefix, then you must specify a subnet mask like 11111111.11111111.11110000.00000000, which uses only 5 bits of the third octet for the extended network prefix.

You can write a subnet mask as a dotted-decimal mask or as a /bits (“slash bits”) mask. In Example 1, for a dotted-decimal mask, you convert each binary octet into a decimal number: 255.255.255.0. For a /bits mask, you add the number of 1s: /24. In Example 2, the decimal number is 255.255.248.0 and the /bits is /21.

You can also supernet multiple Class C networks into a larger network by using part of the third octet for the extended network prefix. For example, 192.168.0.0/20.

Determine the Subnet Mask

See Table 43-1 to determine the subnet mask based on how many hosts you want.

---

**Note**

The first and last number of a subnet are reserved, except for /32, which identifies a single host.
Chapter 43      Addresses, Protocols, and Ports

IPv4 Addresses and Subnet Masks

Table 43-1    Hosts, Bits, and Dotted-Decimal Masks

<table>
<thead>
<tr>
<th>Hosts</th>
<th>/Bits Mask</th>
<th>Dotted-Decimal Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>16,777,216</td>
<td>/8</td>
<td>255.0.0.0 Class A Network</td>
</tr>
<tr>
<td>65,536</td>
<td>/16</td>
<td>255.255.0.0 Class B Network</td>
</tr>
<tr>
<td>32,768</td>
<td>/17</td>
<td>255.255.128.0</td>
</tr>
<tr>
<td>16,384</td>
<td>/18</td>
<td>255.255.192.0</td>
</tr>
<tr>
<td>8192</td>
<td>/19</td>
<td>255.255.224.0</td>
</tr>
<tr>
<td>4096</td>
<td>/20</td>
<td>255.255.240.0</td>
</tr>
<tr>
<td>2048</td>
<td>/21</td>
<td>255.255.248.0</td>
</tr>
<tr>
<td>1024</td>
<td>/22</td>
<td>255.255.252.0</td>
</tr>
<tr>
<td>512</td>
<td>/23</td>
<td>255.255.254.0</td>
</tr>
<tr>
<td>256</td>
<td>/24</td>
<td>255.255.255.0 Class C Network</td>
</tr>
<tr>
<td>128</td>
<td>/25</td>
<td>255.255.255.128</td>
</tr>
<tr>
<td>64</td>
<td>/26</td>
<td>255.255.255.192</td>
</tr>
<tr>
<td>32</td>
<td>/27</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>16</td>
<td>/28</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>8</td>
<td>/29</td>
<td>255.255.255.248</td>
</tr>
<tr>
<td>4</td>
<td>/30</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td>Do not use</td>
<td>/31</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>1</td>
<td>/32</td>
<td>255.255.255.255 Single Host Address</td>
</tr>
</tbody>
</table>

Determining the Address to Use with the Subnet Mask

The following sections describe how to determine the network address to use with a subnet mask for a Class C-size and a Class B-size network.

Class C-Size Network Address

For a network between 2 and 254 hosts, the fourth octet falls on a multiple of the number of host addresses, starting with 0. For example, Table 43-2 shows the 8-host subnets (/29) of 192.168.0.x.

Note

The first and last address of a subnet are reserved. In the first subnet example, you cannot use 192.168.0.0 or 192.168.0.7.

Table 43-2    Class C-Size Network Address

<table>
<thead>
<tr>
<th>Subnet with Mask /29 (255.255.255.248)</th>
<th>Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0</td>
<td>192.168.0.0 to 192.168.0.7</td>
</tr>
<tr>
<td>192.168.0.8</td>
<td>192.168.0.8 to 192.168.0.15</td>
</tr>
<tr>
<td>192.168.0.16</td>
<td>192.168.0.16 to 192.168.0.31</td>
</tr>
</tbody>
</table>
IPv4 Addresses and Subnet Masks

Chapter 43      Addresses, Protocols, and Ports

IPv4 Addresses and Subnet Masks

Class B-Size Network Address

To determine the network address to use with the subnet mask for a network with between 254 and 65,534 hosts, you need to determine the value of the third octet for each possible extended network prefix. For example, you might want to subnet an address like 10.1.x.0, where the first two octets are fixed because they are used in the extended network prefix, and the fourth octet is 0 because all bits are used for the host number.

To determine the value of the third octet, follow these steps:

Step 1  Calculate how many subnets you can make from the network by dividing 65,536 (the total number of addresses using the third and fourth octet) by the number of host addresses you want.

For example, 65,536 divided by 4096 hosts equals 16.

Therefore, there are 16 subnets of 4096 addresses each in a Class B-size network.

Step 2  Determine the multiple of the third octet value by dividing 256 (the number of values for the third octet) by the number of subnets:

In this example, 256/16 = 16.

The third octet falls on a multiple of 16, starting with 0.

Table 43-3 shows the 16 subnets of the network 10.1.

Note  The first and last address of a subnet are reserved. In the first subnet example, you cannot use 10.1.0.0 or 10.1.15.255.

| Table 43-2  Class C-Size Network Address (continued) |
|-----------------------------|-----------------------------|
| Subnet with Mask /29 (255.255.255.248) | Address Range |
| 192.168.0.248 | 192.168.0.248 to 192.168.0.255 |

<table>
<thead>
<tr>
<th>Class B-Size Network Address (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>  Calculate how many subnets you can make from the network by dividing 65,536 (the total number of addresses using the third and fourth octet) by the number of host addresses you want.</td>
</tr>
<tr>
<td>For example, 65,536 divided by 4096 hosts equals 16.</td>
</tr>
<tr>
<td>Therefore, there are 16 subnets of 4096 addresses each in a Class B-size network.</td>
</tr>
<tr>
<td><strong>Step 2</strong>  Determine the multiple of the third octet value by dividing 256 (the number of values for the third octet) by the number of subnets:</td>
</tr>
<tr>
<td>In this example, 256/16 = 16.</td>
</tr>
<tr>
<td>The third octet falls on a multiple of 16, starting with 0.</td>
</tr>
<tr>
<td>Table 43-3 shows the 16 subnets of the network 10.1.</td>
</tr>
<tr>
<td><strong>Note</strong>  The first and last address of a subnet are reserved. In the first subnet example, you cannot use 10.1.0.0 or 10.1.15.255.</td>
</tr>
</tbody>
</table>

| Table 43-3  Subnets of Network |
|-----------------------------|-----------------------------|
| Subnet with Mask /20 (255.255.240.0) | Address Range |
| 10.1.0.0 | 10.1.0.0 to 10.1.15.255 |
| 10.1.16.0 | 10.1.16.0 to 10.1.31.255 |
| 10.1.32.0 | 10.1.32.0 to 10.1.47.255 |
| 10.1.240.0 | 10.1.240.0 to 10.1.255.255 |
IPv6 Addresses

IPv6 is the next generation of the Internet Protocol after IPv4. It provides an expanded address space, a simplified header format, improved support for extensions and options, flow labeling capability, and authentication and privacy capabilities. IPv6 is described in RFC 2460. The IPv6 addressing architecture is described in RFC 3513.

This section describes the IPv6 address format and architecture.

Related Topics
Configuring IPv6 Addressing, page 11-11

IPv6 Address Format

IPv6 addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. The following are two examples of IPv6 addresses:

- 2001:0DB8:0000:0000:0008:0800:200C:417A

Note
The hexadecimal letters in IPv6 addresses are not case-sensitive.

You do not need to include the leading zeros in an individual field of the address, but each field must contain at least one digit. So the example address 2001:0DB8:0000:0000:0008:0800:200C:417A can be shortened to 2001:0DB8:0:0:8:800:200C:417A by removing the leading zeros from the third through sixth fields from the left. The fields that contained all zeros (the third and fourth fields from the left) were shortened to a single zero. The fifth field from the left had the three leading zeros removed, leaving a single 8 in that field, and the sixth field from the left had the one leading zero removed, leaving 800 in that field.

It is common for IPv6 addresses to contain several consecutive hexadecimal fields of zeros. You can use two colons (::) to compress consecutive fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent the successive hexadecimal fields of zeros). Table 43-4 shows several examples of address compression for different types of IPv6 address.

Table 43-4 IPv6 Address Compression Examples

<table>
<thead>
<tr>
<th>Address Type</th>
<th>Standard Form</th>
<th>Compressed Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast</td>
<td>2001:0DB8:0:0:BA98:0:3210</td>
<td>2001:0DB8::BA98:0:3210</td>
</tr>
<tr>
<td>Multicast</td>
<td>FF01:0:0:0:0:0:0:101</td>
<td>FF01::101</td>
</tr>
<tr>
<td>Loopback</td>
<td>0:0:0:0:0:0:0:1</td>
<td>::1</td>
</tr>
<tr>
<td>Unspecified</td>
<td>0:0:0:0:0:0:0:0</td>
<td>::</td>
</tr>
</tbody>
</table>

Note
Two colons (::) can be used only once in an IPv6 address to represent successive fields of zeros.
An alternative form of the IPv6 format is often used when dealing with an environment that contains both IPv4 and IPv6 addresses. This alternative has the format x:x:x:x:x:y.y.y, where x represent the hexadecimal values for the six high-order parts of the IPv6 address and y represent decimal values for the 32-bit IPv4 part of the address (which takes the place of the remaining two 16-bit parts of the IPv6 address). For example, the IPv4 address 192.168.1.1 could be represented as the IPv6 address 0:0:0:0:0:0:FFFF:192.168.1.1 or ::FFFF:192.168.1.1.

**IPv6 Address Types**

The following are the three main types of IPv6 addresses:

- **Unicast**—A unicast address is an identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address. An interface may have more than one unicast address assigned to it.

- **Multicast**—A multicast address is an identifier for a set of interfaces. A packet sent to a multicast address is delivered to all addresses identified by that address.

- **Anycast**—An anycast address is an identifier for a set of interfaces. Unlike a multicast address, a packet sent to an anycast address is only delivered to the “nearest” interface, as determined by the measure of distances for the routing protocol.

---

**Note**

There are no broadcast addresses in IPv6. Multicast addresses provide the broadcast functionality.

**Unicast Addresses**

This section describes IPv6 unicast addresses. Unicast addresses identify an interface on a network node.

**Global Address**

The general format of an IPv6 global unicast address is a global routing prefix followed by a subnet ID followed by an interface ID. The global routing prefix can be any prefix not reserved by another IPv6 address type.

All global unicast addresses, other than those that start with binary 000, have a 64-bit interface ID in the Modified EUI-64 format.

Global unicast address that start with the binary 000 do not have any constraints on the size or structure of the interface ID portion of the address. One example of this type of address is an IPv6 address with an embedded IPv4 address.

**Related Topics**

- IPv6 Address Prefixes, page 43-10
- Interface Identifiers, page 43-8
- IPv4-Compatible IPv6 Addresses, page 43-7

**Site-Local Address**

Site-local addresses are used for addressing within a site. They can be used to address an entire site without using a globally unique prefix. Site-local addresses have the prefix FEC0::/10, followed by a 54-bit subnet ID, and end with a 64-bit interface ID in the modified EUI-64 format.
Site-local routers do not forward any packets that have a site-local address for a source or destination outside of the site. Therefore, site-local addresses can be considered private addresses.

**Link-Local Address**

All interfaces are required to have at least one link-local address. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 and the interface identifier in modified EUI-64 format. Link-local addresses are used in the neighbor discovery protocol and the stateless autoconfiguration process. Nodes with a link-local address can communicate; they do not need a site-local or globally unique address to communicate.

Routers do not forward any packets that have a link-local address for a source or destination. Therefore, link-local addresses can be considered private addresses.

**IPv4-Compatible IPv6 Addresses**

There are two types of IPv6 addresses that can contain IPv4 addresses.

The first type is the IPv4-compatibly IPv6 address. The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits. This type of address is termed an IPv4-compatible IPv6 address and has the format ::y.y.y.y, where y.y.y.y is an IPv4 unicast address.

*Note* The IPv4 address used in the IPv4-compatible IPv6 address must be a globally unique IPv4 unicast address.

The second type of IPv6 address, which holds an embedded IPv4 address, is called the IPv4-mapped IPv6 address. This address type is used to represent the addresses of IPv4 nodes as IPv6 addresses. This type of address has the format ::FFFF:y.y.y.y, where y.y.y.y is an IPv4 unicast address.

**Unspecified Address**

The unspecified address, 0:0:0:0:0:0:0:0, indicates the absence of an IPv6 address. For example, a newly initialized node on an IPv6 network may use the unspecified address as the source address in its packets until it receives its IPv6 address.

*Note* The IPv6 unspecified address cannot be assigned to an interface. The unspecified IPv6 addresses must not be used as destination addresses in IPv6 packets or the IPv6 routing header.

**Loopback Address**

The loopback address, 0:0:0:0:0:0:0:1, may be used by a node to send an IPv6 packet to itself. The loopback address in IPv6 functions the same as the loopback address in IPv4 (127.0.0.1).
The IPv6 loopback address cannot be assigned to a physical interface. A packet that has the IPv6 loopback address as its source or destination address must remain within the node that created the packet. IPv6 routers do not forward packets that have the IPv6 loopback address as their source or destination address.

### Interface Identifiers

Interface identifiers in IPv6 unicast addresses are used to identify the interfaces on a link. They need to be unique within a subnet prefix. In many cases, the interface identifier is derived from the interface link-layer address. The same interface identifier may be used on multiple interfaces of a single node, as long as those interfaces are attached to different subnets.

For all unicast addresses, except those that start with the binary 000, the interface identifier is required to be 64 bits long and to be constructed in the Modified EUI-64 format. The Modified EUI-64 format is created from the 48-bit MAC address by inverting the universal/local bit in the address and by inserting the hexadecimal number FFFE between the upper three bytes and lower three bytes of the of the MAC address.

For example, and interface with the MAC address of 00E0.b601.3B7A would have a 64-bit interface ID of 02E0:B6FF:FE01:3B7A.

### Multicast Address

An IPv6 multicast address is an identifier for a group of interfaces, typically on different nodes. A packet sent to a multicast address is delivered to all interfaces identified by the multicast address. An interface may belong to any number of multicast groups.

An IPv6 multicast address has a prefix of FF00::/8 (1111 1111). The octet following the prefix defines the type and scope of the multicast address. A permanently assigned (well known) multicast address has a flag parameter equal to 0; a temporary (transient) multicast address has a flag parameter equal to 1. A multicast address that has the scope of a node, link, site, or organization, or a global scope has a scope parameter of 1, 2, 5, 8, or E, respectively. For example, a multicast address with the prefix FF02::/16 is a permanent multicast address with a link scope. Figure 43-1 shows the format of the IPv6 multicast address.

![IPv6 Multicast Address Format](image-url)
IPv6 nodes (hosts and routers) are required to join the following multicast groups:

- The All Nodes multicast addresses:
  - FF01:: (interface-local)
  - FF02:: (link-local)

- The Solicited-Node Address for each IPv6 unicast and anycast address on the node: FF02:0:0:0:0:1:FFXX:XXXX/104, where XX:XXXX is the low-order 24-bits of the unicast or anycast address.

  **Note** Solicited-Node addresses are used in Neighbor Solicitation messages.

IPv6 routers are required to join the following multicast groups:

- FF01::2 (interface-local)
- FF02::2 (link-local)
- FF05::2 (site-local)

Multicast address should not be used as source addresses in IPv6 packets.

  **Note** There are no broadcast addresses in IPv6. IPv6 multicast addresses are used instead of broadcast addresses.

### Anycast Address

The IPv6 anycast address is a unicast address that is assigned to more than one interface (typically belonging to different nodes). A packet that is routed to an anycast address is routed to the nearest interface having that address, the nearness being determined by the routing protocol in effect.

Anycast addresses are allocated from the unicast address space. An anycast address is simply a unicast address that has been assigned to more than one interface, and the interfaces must be configured to recognize the address as an anycast address.

The following restrictions apply to anycast addresses:

- An anycast address cannot be used as the source address for an IPv6 packet.
- An anycast address cannot be assigned to an IPv6 host; it can only be assigned to an IPv6 router.

  **Note** Anycast addresses are not supported on the ASA.

### Required Addresses

IPv6 hosts must, at a minimum, be configured with the following addresses (either automatically or manually):

- A link-local address for each interface
- The loopback address
- The All-Nodes multicast addresses
- A Solicited-Node multicast address for each unicast or anycast address
IPv6 routers must, at a minimum, be configured with the following addresses (either automatically or manually):

- The required host addresses
- The Subnet-Router anycast addresses for all interfaces for which it is configured to act as a router
- The All-Routers multicast addresses

**IPv6 Address Prefixes**

An IPv6 address prefix, in the format ipv6-prefix/prefix-length, can be used to represent bit-wise contiguous blocks of the entire address space. The IPv6-prefix must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:0DB8:8086:6502::/32 is a valid IPv6 prefix.

The IPv6 prefix identifies the type of IPv6 address. **Table 43-5** shows the prefixes for each IPv6 address type.

<table>
<thead>
<tr>
<th>Address Type</th>
<th>Binary Prefix</th>
<th>IPv6 Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unspecified</td>
<td>000...0 (128 bits)</td>
<td>::/128</td>
</tr>
<tr>
<td>Loopback</td>
<td>000...1 (128 bits)</td>
<td>::1/128</td>
</tr>
<tr>
<td>Multicast</td>
<td>11111111</td>
<td>FF00::/8</td>
</tr>
<tr>
<td>Link-Local (unicast)</td>
<td>1111111010</td>
<td>FE80::/10</td>
</tr>
<tr>
<td>Site-Local (unicast)</td>
<td>11111111111</td>
<td>FEC0::/10</td>
</tr>
<tr>
<td>Global (unicast)</td>
<td>All other addresses.</td>
<td></td>
</tr>
<tr>
<td>Anycast</td>
<td>Taken from the unicast address space.</td>
<td></td>
</tr>
</tbody>
</table>

**Protocols and Applications**

**Table 43-6** lists the protocol literal values and port numbers; either can be entered in ASA commands.

<table>
<thead>
<tr>
<th>Literal</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ah</td>
<td>51</td>
<td>Authentication Header for IPv6, RFC 1826.</td>
</tr>
<tr>
<td>esp</td>
<td>50</td>
<td>Encapsulated Security Payload for IPv6, RFC 1827.</td>
</tr>
<tr>
<td>gre</td>
<td>47</td>
<td>Generic Routing Encapsulation.</td>
</tr>
<tr>
<td>icmp</td>
<td>1</td>
<td>Internet Control Message Protocol, RFC 792.</td>
</tr>
<tr>
<td>icmp6</td>
<td>58</td>
<td>Internet Control Message Protocol for IPv6, RFC 2463.</td>
</tr>
<tr>
<td>igmp</td>
<td>2</td>
<td>Internet Group Management Protocol, RFC 1112.</td>
</tr>
<tr>
<td>igrp</td>
<td>9</td>
<td>Interior Gateway Routing Protocol.</td>
</tr>
</tbody>
</table>
TCP and UDP Ports

Table 43-7 lists the literal values and port numbers; either can be entered in ASA commands. See the following caveats:

- The ASA uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net. This value, however, does not agree with IANA port assignments.

- The ASA listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses the standard ports 1812 and 1813, you can configure the ASA to listen to those ports using the `authentication-port` and `accounting-port` commands.

- To assign a port for DNS access, use the `domain` literal value, not `dns`. If you use `dns`, the ASA assumes you meant to use the `dnisix` literal value.

You can view port numbers online at the IANA website:

http://www.iana.org/assignments/port-numbers
### Table 43-7 Port Literal Values (continued)

<table>
<thead>
<tr>
<th>Literal</th>
<th>TCP or UDP?</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootps</td>
<td>UDP</td>
<td>67</td>
<td>Bootstrap Protocol Server</td>
</tr>
<tr>
<td>chargen</td>
<td>TCP</td>
<td>19</td>
<td>Character Generator</td>
</tr>
<tr>
<td>citrix-ica</td>
<td>TCP</td>
<td>1494</td>
<td>Citrix Independent Computing Architecture (ICA) protocol</td>
</tr>
<tr>
<td>cmd</td>
<td>TCP</td>
<td>514</td>
<td>Similar to <code>exec</code> except that <code>cmd</code> has automatic authentication</td>
</tr>
<tr>
<td>ctiqbe</td>
<td>TCP</td>
<td>2748</td>
<td>Computer Telephony Interface Quick Buffer Encoding</td>
</tr>
<tr>
<td>daytime</td>
<td>TCP</td>
<td>13</td>
<td>Day time, RFC 867</td>
</tr>
<tr>
<td>discard</td>
<td>TCP, UDP</td>
<td>9</td>
<td>Discard</td>
</tr>
<tr>
<td>domain</td>
<td>TCP, UDP</td>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>dnsix</td>
<td>UDP</td>
<td>195</td>
<td>DNSIX Session Management Module Audit Redirector</td>
</tr>
<tr>
<td>echo</td>
<td>TCP, UDP</td>
<td>7</td>
<td>Echo</td>
</tr>
<tr>
<td>exec</td>
<td>TCP</td>
<td>512</td>
<td>Remote process execution</td>
</tr>
<tr>
<td>finger</td>
<td>TCP</td>
<td>79</td>
<td>Finger</td>
</tr>
<tr>
<td>ftp</td>
<td>TCP</td>
<td>21</td>
<td>File Transfer Protocol (control port)</td>
</tr>
<tr>
<td>ftp-data</td>
<td>TCP</td>
<td>20</td>
<td>File Transfer Protocol (data port)</td>
</tr>
<tr>
<td>gopher</td>
<td>TCP</td>
<td>70</td>
<td>Gopher</td>
</tr>
<tr>
<td>https</td>
<td>TCP</td>
<td>443</td>
<td>HTTP over SSL</td>
</tr>
<tr>
<td>h323</td>
<td>TCP</td>
<td>1720</td>
<td>H.323 call signaling</td>
</tr>
<tr>
<td>hostname</td>
<td>TCP</td>
<td>101</td>
<td>NIC Host Name Server</td>
</tr>
<tr>
<td>ident</td>
<td>TCP</td>
<td>113</td>
<td>Identiﬁcation authentication service</td>
</tr>
<tr>
<td>imap4</td>
<td>TCP</td>
<td>143</td>
<td>Internet Message Access Protocol, version 4</td>
</tr>
<tr>
<td>irc</td>
<td>TCP</td>
<td>194</td>
<td>Internet Relay Chat protocol</td>
</tr>
<tr>
<td>isakmp</td>
<td>UDP</td>
<td>500</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>kerberos</td>
<td>TCP, UDP</td>
<td>750</td>
<td>Kerberos</td>
</tr>
<tr>
<td>klogin</td>
<td>TCP</td>
<td>543</td>
<td>KLOGIN</td>
</tr>
<tr>
<td>kshell</td>
<td>TCP</td>
<td>544</td>
<td>Korn Shell</td>
</tr>
<tr>
<td>ldap</td>
<td>TCP</td>
<td>389</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>ldaps</td>
<td>TCP</td>
<td>636</td>
<td>Lightweight Directory Access Protocol (SSL)</td>
</tr>
<tr>
<td>lpd</td>
<td>TCP</td>
<td>515</td>
<td>Line Printer Daemon - printer spooler</td>
</tr>
<tr>
<td>login</td>
<td>TCP</td>
<td>513</td>
<td>Remote login</td>
</tr>
<tr>
<td>lotusnotes</td>
<td>TCP</td>
<td>1352</td>
<td>IBM Lotus Notes</td>
</tr>
<tr>
<td>mobile-ip</td>
<td>UDP</td>
<td>434</td>
<td>Mobile IP-Agent</td>
</tr>
<tr>
<td>nameserver</td>
<td>UDP</td>
<td>42</td>
<td>Host Name Server</td>
</tr>
</tbody>
</table>
Table 43-7  Port Literal Values (continued)

<table>
<thead>
<tr>
<th>Literal</th>
<th>TCP or UDP?</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>netbios-ns</td>
<td>UDP</td>
<td>137</td>
<td>NetBIOS Name Service</td>
</tr>
<tr>
<td>netbios-dgm</td>
<td>UDP</td>
<td>138</td>
<td>NetBIOS Datagram Service</td>
</tr>
<tr>
<td>netbios-ssn</td>
<td>TCP</td>
<td>139</td>
<td>NetBIOS Session Service</td>
</tr>
<tr>
<td>nntp</td>
<td>TCP</td>
<td>119</td>
<td>Network News Transfer Protocol</td>
</tr>
<tr>
<td>ntp</td>
<td>UDP</td>
<td>123</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>pcanywhere-status</td>
<td>UDP</td>
<td>5632</td>
<td>pcAnywhere status</td>
</tr>
<tr>
<td>pcanywhere-data</td>
<td>TCP</td>
<td>5631</td>
<td>pcAnywhere data</td>
</tr>
<tr>
<td>pim-auto-rp</td>
<td>TCP, UDP</td>
<td>496</td>
<td>Protocol Independent Multicast, reverse path flooding, dense mode</td>
</tr>
<tr>
<td>pop2</td>
<td>TCP</td>
<td>109</td>
<td>Post Office Protocol - Version 2</td>
</tr>
<tr>
<td>pop3</td>
<td>TCP</td>
<td>110</td>
<td>Post Office Protocol - Version 3</td>
</tr>
<tr>
<td>pppp</td>
<td>TCP</td>
<td>1723</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>radius</td>
<td>UDP</td>
<td>1645</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>radius-acct</td>
<td>UDP</td>
<td>1646</td>
<td>Remote Authentication Dial-In User Service (accounting)</td>
</tr>
<tr>
<td>rip</td>
<td>UDP</td>
<td>520</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>secureid-udp</td>
<td>UDP</td>
<td>5510</td>
<td>SecureID over UDP</td>
</tr>
<tr>
<td>smtp</td>
<td>TCP</td>
<td>25</td>
<td>Simple Mail Transport Protocol</td>
</tr>
<tr>
<td>snmp</td>
<td>UDP</td>
<td>161</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>snmptrap</td>
<td>UDP</td>
<td>162</td>
<td>Simple Network Management Protocol - Trap</td>
</tr>
<tr>
<td>sqlnet</td>
<td>TCP</td>
<td>1521</td>
<td>Structured Query Language Network</td>
</tr>
<tr>
<td>ssh</td>
<td>TCP</td>
<td>22</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>sunrpc (rpc)</td>
<td>TCP, UDP</td>
<td>111</td>
<td>Sun Remote Procedure Call</td>
</tr>
<tr>
<td>syslog</td>
<td>UDP</td>
<td>514</td>
<td>System Log</td>
</tr>
<tr>
<td>tacacs</td>
<td>TCP, UDP</td>
<td>49</td>
<td>Terminal Access Controller Access Control System Plus</td>
</tr>
<tr>
<td>talk</td>
<td>TCP, UDP</td>
<td>517</td>
<td>Talk</td>
</tr>
<tr>
<td>telnet</td>
<td>TCP</td>
<td>23</td>
<td>RFC 854 Telnet</td>
</tr>
<tr>
<td>tftp</td>
<td>UDP</td>
<td>69</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>time</td>
<td>UDP</td>
<td>37</td>
<td>Time</td>
</tr>
<tr>
<td>uucp</td>
<td>TCP</td>
<td>540</td>
<td>UNIX-to-UNIX Copy Program</td>
</tr>
<tr>
<td>who</td>
<td>UDP</td>
<td>513</td>
<td>Who</td>
</tr>
<tr>
<td>whois</td>
<td>TCP</td>
<td>43</td>
<td>Who Is</td>
</tr>
<tr>
<td>www</td>
<td>TCP</td>
<td>80</td>
<td>World Wide Web</td>
</tr>
<tr>
<td>xdmcp</td>
<td>UDP</td>
<td>177</td>
<td>X Display Manager Control Protocol</td>
</tr>
</tbody>
</table>
Local Ports and Protocols

Table 43-8 lists the protocols, TCP ports, and UDP ports that the ASA may open to process traffic destined to the ASA. Unless you enable the features and services listed in Table 43-8, the ASA does not open any local protocols or any TCP or UDP ports. You must configure a feature or service for the ASA to open the default listening protocol or port. In many cases you can configure ports other than the default port when you enable a feature or service.

Table 43-8 Protocols and Ports Opened by Features and Services

<table>
<thead>
<tr>
<th>Feature or Service</th>
<th>Protocol</th>
<th>Port Number</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>UDP</td>
<td>67,68</td>
<td></td>
</tr>
<tr>
<td>Failover Control</td>
<td>105</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>1</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>IGMP</td>
<td>2</td>
<td>N/A</td>
<td>Protocol only open on destination IP address 224.0.0.1</td>
</tr>
<tr>
<td>ISAKMP/IKE</td>
<td>UDP</td>
<td>500</td>
<td>Configurable.</td>
</tr>
<tr>
<td>IPsec (ESP)</td>
<td>50</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>IPsec over UDP (NAT-T)</td>
<td>UDP</td>
<td>4500</td>
<td></td>
</tr>
<tr>
<td>IPsec over UDP (Cisco VPN 3000 Series compatible)</td>
<td>UDP</td>
<td>10000</td>
<td>Configurable.</td>
</tr>
<tr>
<td>IPsec over TCP (CTCP)</td>
<td>TCP</td>
<td>—</td>
<td>No default port is used. You must specify the port number when configuring IPsec over TCP.</td>
</tr>
<tr>
<td>NTP</td>
<td>UDP</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>89</td>
<td>N/A</td>
<td>Protocol only open on destination IP address 224.0.0.5 and 224.0.0.6</td>
</tr>
<tr>
<td>PIM</td>
<td>103</td>
<td>N/A</td>
<td>Protocol only open on destination IP address 224.0.0.13</td>
</tr>
<tr>
<td>RIP</td>
<td>UDP</td>
<td>520</td>
<td></td>
</tr>
<tr>
<td>RIPv2</td>
<td>UDP</td>
<td>520</td>
<td>Port only open on destination IP address 224.0.0.9</td>
</tr>
<tr>
<td>SNMP</td>
<td>UDP</td>
<td>161</td>
<td>Configurable.</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Stateful Update</td>
<td>8 (non-secure)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>TCP</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>UDP</td>
<td>9023</td>
<td>Configurable.</td>
</tr>
<tr>
<td>VPN Individual User Authentication Proxy</td>
<td>UDP</td>
<td>1645, 1646</td>
<td>Port accessible only over VPN tunnel.</td>
</tr>
</tbody>
</table>
ICMP Types

Table 43-9 lists the ICMP type numbers and names that you can enter in ASA commands.

<table>
<thead>
<tr>
<th>ICMP Number</th>
<th>ICMP Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>echo-reply</td>
</tr>
<tr>
<td>3</td>
<td>unreachable</td>
</tr>
<tr>
<td>4</td>
<td>source-quench</td>
</tr>
<tr>
<td>5</td>
<td>redirect</td>
</tr>
<tr>
<td>6</td>
<td>alternate-address</td>
</tr>
<tr>
<td>8</td>
<td>echo</td>
</tr>
<tr>
<td>9</td>
<td>router-advertisement</td>
</tr>
<tr>
<td>10</td>
<td>router-solicitation</td>
</tr>
<tr>
<td>11</td>
<td>time-exceeded</td>
</tr>
<tr>
<td>12</td>
<td>parameter-problem</td>
</tr>
<tr>
<td>13</td>
<td>timestamp-request</td>
</tr>
<tr>
<td>14</td>
<td>timestamp-reply</td>
</tr>
<tr>
<td>15</td>
<td>information-request</td>
</tr>
<tr>
<td>16</td>
<td>information-reply</td>
</tr>
<tr>
<td>17</td>
<td>mask-request</td>
</tr>
<tr>
<td>18</td>
<td>mask-reply</td>
</tr>
<tr>
<td>31</td>
<td>conversion-error</td>
</tr>
<tr>
<td>32</td>
<td>mobile-redirect</td>
</tr>
</tbody>
</table>