CHAPTER 8

Configuring a Cluster of ASAs

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 the "Unsupported Features" section on page 8-20.

Information About ASA Clustering

- Inter-Site Clustering, page 8-16
- How the ASA Cluster Manages Connections, page 8-18
- ASA Features and Clustering, page 8-20

How the ASA Cluster Fits into Your Network

The cluster consists of multiple ASAs acting as a single unit. (See the "Licensing Requirements for ASA Clustering" section on page 8-27 for the number of units supported per model). 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*. See the "Cluster Control Link" section on page 8-6.
- Management access to each ASA for configuration and monitoring. See the "ASA Cluster Management" section on page 8-11.

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. See the "Spanned EtherChannel (Recommended)" section on page 8-13.
- Policy-Based Routing (Routed firewall mode only)—The upstream and downstream routers perform load balancing between units using route maps and ACLs. See the "Policy-Based Routing (Routed Firewall Mode Only)" section on page 8-15.
- 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. See the "Equal-Cost Multi-Path Routing (Routed Firewall Mode Only)" section on page 8-16.

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

- ASA Hardware and Software Requirements, page 8-3
- Bootstrap Configuration, page 8-3
- Master and Slave Unit Roles, page 8-3
- Master Unit Election, page 8-3

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. See the "Upgrade Path and Migrations" section on page 42-1.
- (9.1.3 and Earlier) Must be in the same geographical location. (9.1(4) and later) You can have cluster members in different geographical locations (inter-site) when using individual interface mode. See the "Inter-Site Clustering" section on page 8-16 for more information.
- 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.

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. See the "Centralized Features" section on page 8-21.

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. See the "Centralized Features" section on page 8-21 for a list of centralized features.

ASA Cluster Interfaces

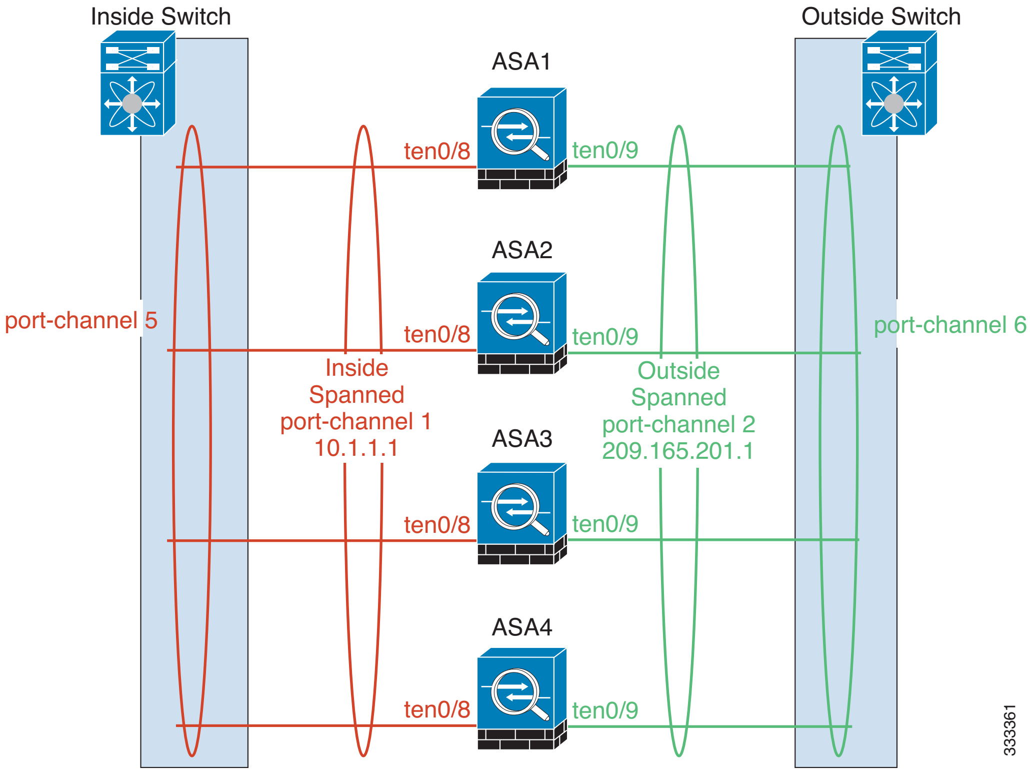
You can configure data interfaces as either Spanned EtherChannels or as Individual interfaces. All data interfaces in the cluster must be one type only.

- Interface Types, page 8-4
- Interface Type Mode, page 8-6

Interface Types

- Spanned EtherChannel (Recommended)

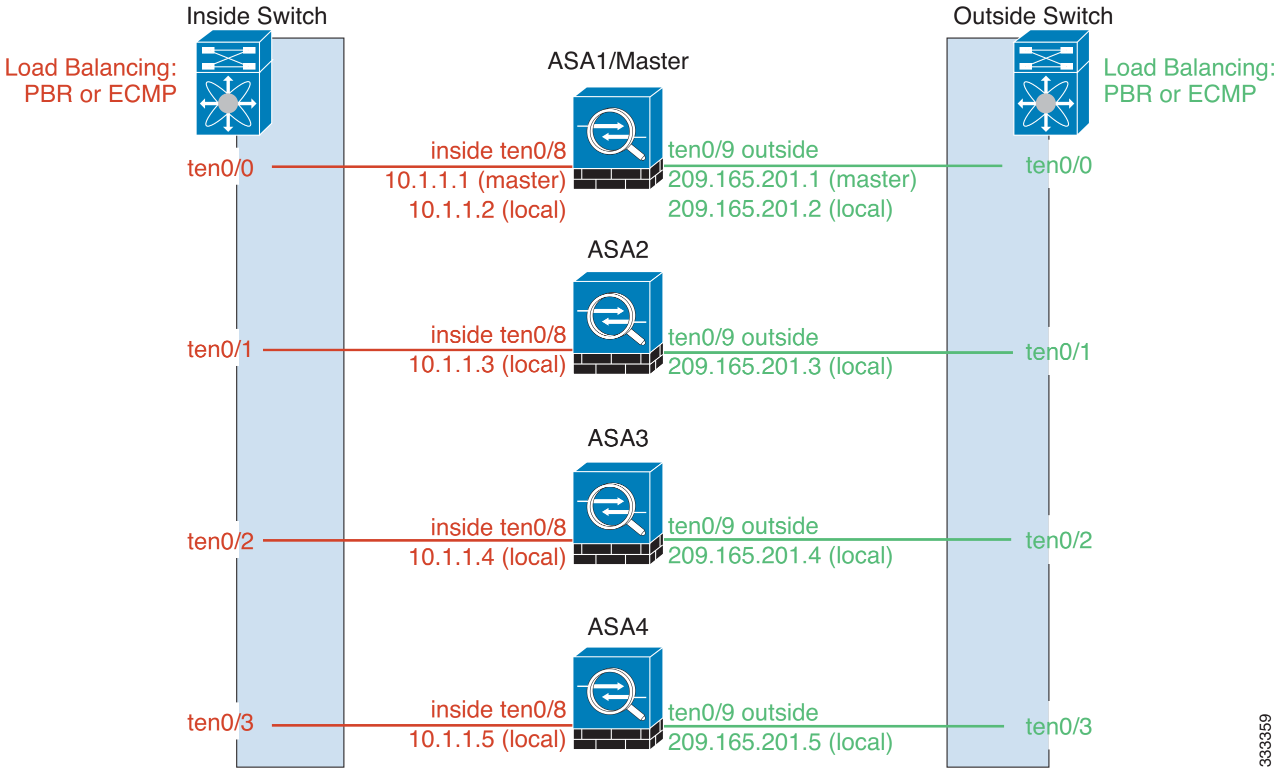
  You can group one or more interfaces per unit into an EtherChannel that spans all units in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel. A Spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed 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. See also the "Spanned EtherChannel (Recommended)" section on page 8-13.



- 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. For information about load balancing, see the "Load Balancing Methods" section on page 8-13.

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.



Interface Type Mode

You must choose the interface type (Spanned EtherChannel or Individual) before you configure your devices. See the following guidelines for the interface type mode:

- 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.

Cluster Control Link

Each unit must dedicate at least one hardware interface as the cluster control link.

- Cluster Control Link Traffic Overview, page 8-7
- Cluster Control Link Interfaces and Network, page 8-7
- Sizing the Cluster Control Link, page 8-7
- Cluster Control Link Redundancy, page 8-8

- Cluster Control Link Reliability, page 8-8
- Cluster Control Link Failure, page 8-9

Cluster Control Link Traffic Overview

Cluster control link traffic includes both control and data traffic.

Control traffic includes:

- Master election. (See the "Cluster Members" section on page 8-2.)
- Configuration replication. (See the "Configuration Replication" section on page 8-11.)
- Health monitoring. (See the "Unit Health Monitoring" section on page 8-9.)

Data traffic includes:

- State replication. (See the "Data Path Connection State Replication" section on page 8-10.)
- Connection ownership queries and data packet forwarding. (See the "Rebalancing New TCP Connections Across the Cluster" section on page 8-20.)

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; see the "Cluster Control Link Redundancy" section on page 8-8 for more information.

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. See the "Sizing the Cluster Control Link" section on page 8-7 for more information.

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.

Sizing 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.

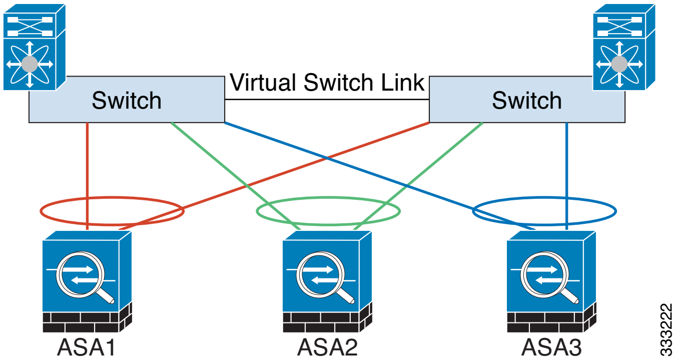
Note If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

(9.1(4) and later) For inter-site clusters and sizing the data center interconnect for cluster control link traffic, see the "Inter-Site Clustering" section on page 8-16.

Cluster Control Link Redundancy

We recommend using an EtherChannel for the cluster control link, so 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

(9.1(4) and later) 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; see Rejoining the Cluster, page 8-10.

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.

High Availability within the ASA Cluster

- 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 an interface fails on a particular unit, but the same interface is active 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. If the unit is joining the cluster as a new member, the ASA waits 45 seconds before rejecting the new unit. 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; see Rejoining the Cluster, page 8-10.

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.

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** (see Configuring Basic Bootstrap Settings and Enabling Clustering, page 8-45).
- 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** (see Configuring Basic Bootstrap Settings and Enabling Clustering, page 8-45).
- 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.

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 Table 8-1 for clustering support or lack of support for this kind of traffic.

Table 8-1 ASA Features Replicated Across the Cluster

Traffic	State Support	Notes
Up time	Yes	Keeps track of the system up time.
ARP Table	Yes	Transparent mode only.
MAC address table	Yes	Transparent mode only.
User Identity	Yes	Includes AAA rules (uauth) and identify firewall.
IPv6 Neighbor database	Yes	
Dynamic routing	Yes	
SNMP Engine ID	**No**	
VPN (Site-to-Site)	**No**	VPN sessions will be disconnected if the master unit fails.

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

- 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.

Note 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 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 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. For more information, see Chapter 40, "Configuring Digital Certificates."

Load Balancing Methods

See also the "ASA Cluster Interfaces" section on page 8-4.

- Spanned EtherChannel (Recommended), page 8-13
- Policy-Based Routing (Routed Firewall Mode Only), page 8-15
- Equal-Cost Multi-Path Routing (Routed Firewall Mode Only), page 8-16

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 8-14
- 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.

For more information about EtherChannels in general (not just for clustering), see the "EtherChannels" section on 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 (see the "Customizing the EtherChannel" section on page 9-32). On the switch, we recommend that you use one of the following algorithms: **source-dest-ip** or **source-dest-ip-port** (see the Nexus OS or 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. See the "Load Balancing" section on page 9-7 for more information.

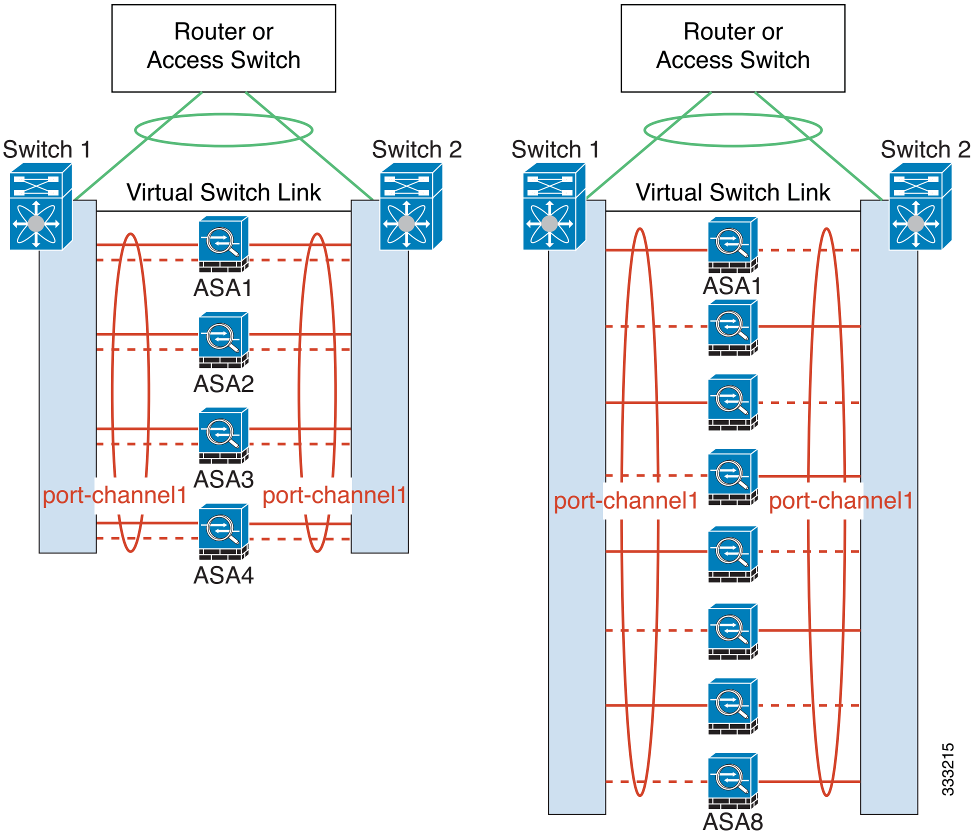
Symmetric load balancing is not always possible. If you configure NAT, then forward and return packets will have different IP addresses and/or ports. Return traffic will be sent to a different unit based on the hash, and the cluster will have to redirect most returning traffic to the correct unit. See the "NAT" section on page 8-24 for more information.

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. Keep in mind that an EtherChannel can have only 8 active interfaces out of 16 maximum; the remaining 8 interfaces are on standby in case of link failure. The following figure shows a 4-ASA cluster and an 8-ASA cluster, both with a total of 16 links in the EtherChannel. 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 IOS PBR with Object Tracking. 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 URLs for more details:

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtpbrtrk.html#wp1057830

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

9.1(4) and later

- Inter-Site Clustering Guidelines, page 8-16
- Sizing the Data Center Interconnect, page 8-17
- Inter-Site Example, page 8-17

Inter-Site Clustering Guidelines

See the following guidelines for inter-site clustering:

- Individual Interface mode only.
- 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 (see the "Rebalancing New TCP Connections Across the Cluster" section on page 8-20); 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 (see the "Connection Roles" section on page 8-18). This is expected behavior.

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:

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

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

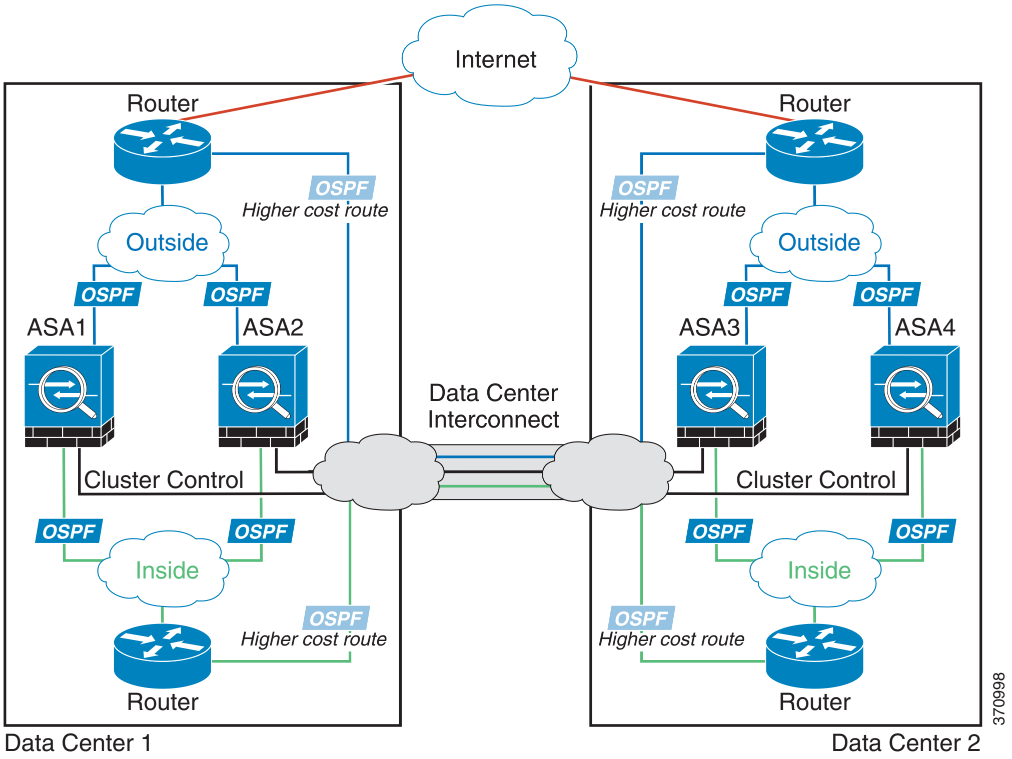
  Reserved DCI bandwidth = 10 Gbps (4/2 x 5 Gbps).
- For 6 members at 3 sites:
  - 6 cluster members total
  - 3 members at site 1, 2 members at site 2, and 1 member at site 3
  - 10 Gbps cluster control link per member

  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 Example

The following example shows 2 ASA cluster members at each of 2 data centers. 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.



How the ASA Cluster Manages Connections

- Connection Roles, page 8-18
- New Connection Ownership, page 8-19
- Sample Data Flow, page 8-19
- Rebalancing New TCP Connections Across the Cluster, page 8-20

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.

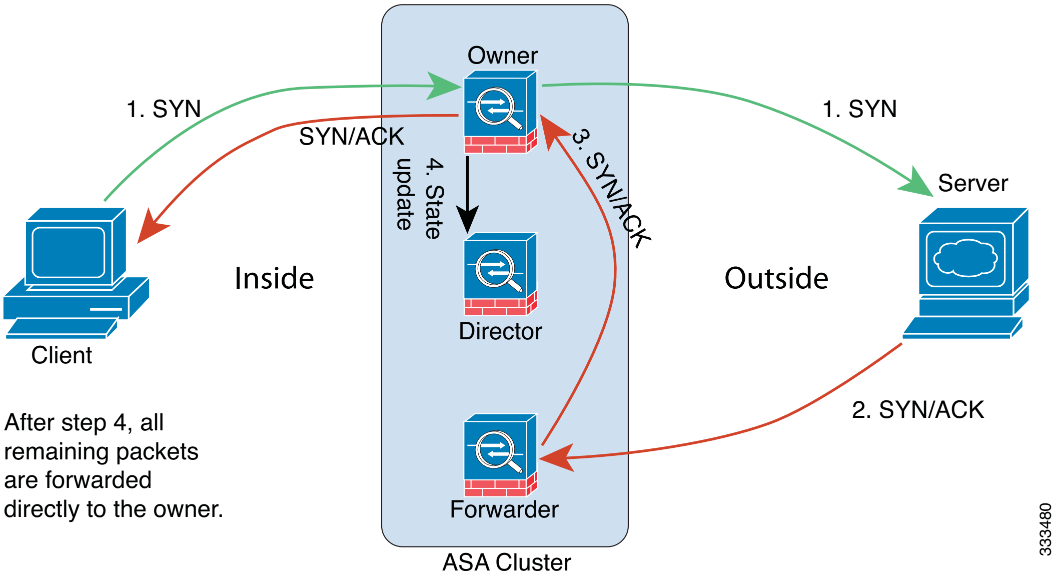
- Forwarder—A unit that forwards packets to the owner. If a forwarder receives a packet for a connection it does not own, it queries the director for the owner, and then establishes a flow to the owner for any other packets it receives for this connection. The director can also be a forwarder. Note that 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. For more information, see the "Load Balancing Methods" section on page 8-13.

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

Unsupported Features

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

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; see the "Sizing the Cluster Control Link" section on page 8-7 to ensure adequate bandwidth for the cluster control link.

If you use the rebalancing feature (see the "Rebalancing New TCP Connections Across the Cluster" section on page 8-20), 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

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.
- 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.

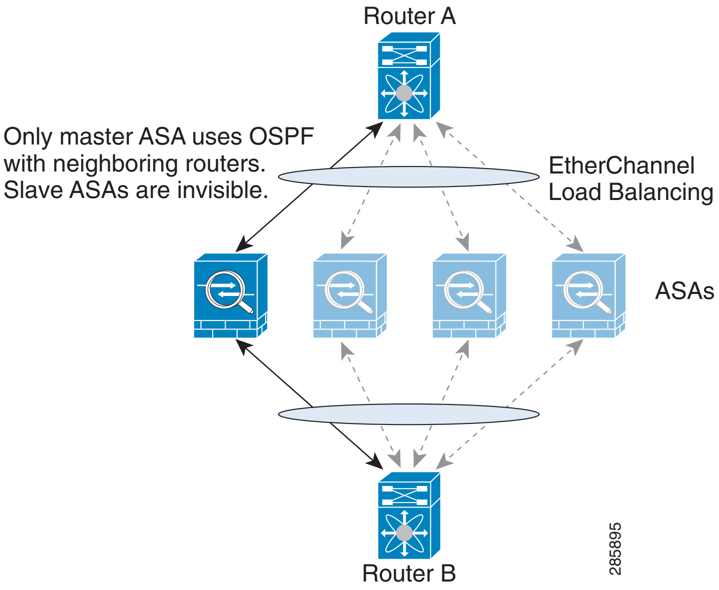
Dynamic Routing

- Dynamic Routing in Spanned EtherChannel Mode, page 8-22
- Dynamic Routing in Individual Interface Mode, page 8-23

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.

Figure 8-1 Dynamic Routing in Spanned EtherChannel Mode


Router A
Only master ASA uses OSPF with neighboring routers. Slave ASAs are invisible.
EtherChannel Load Balancing
ASAs
Router B
285895

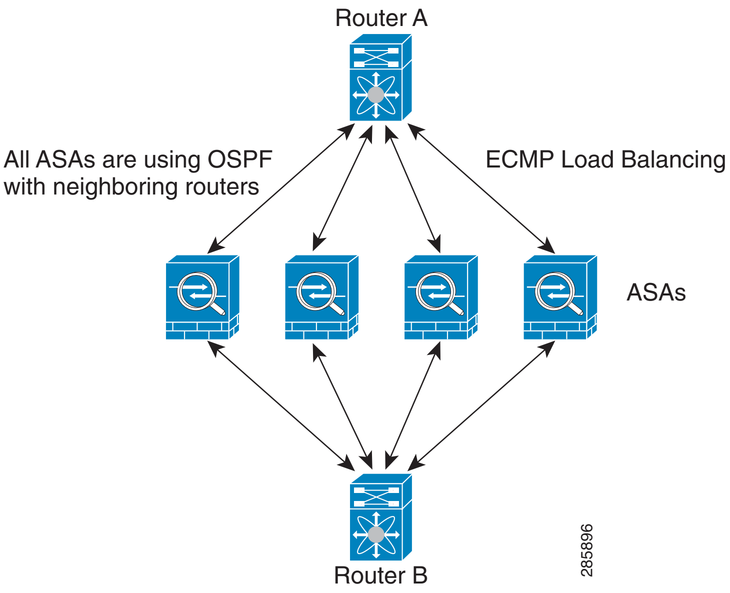
After the slave members learn the routes from the master unit, each unit makes forwarding decisions independently.

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.

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.

Figure 8-2 Dynamic Routing in Individual Interface Mode



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

- Multicast Routing in Spanned EtherChannel Mode, page 8-24
- Multicast Routing in Individual Interface Mode, page 8-24

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

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 xlates managed by the master unit—The master unit maintains and replicates the xlate table to slave units. When a slave unit receives a connection that requires dynamic NAT, and the xlate is not in the table, it requests the xlate 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 xlate. 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 Per-Session PAT vs. Multi-Session PAT section in 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

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

- 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. See the "Including the Device ID in Non-EMBLEM Format Syslog Messages" section on page 44-18.
- NetFlow—Each unit in the cluster generates its own NetFlow stream. The NetFlow collector can only treat each ASA as a separate NetFlow exporter.

SNMP

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

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

- 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

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 Requirements for ASA Clustering

Model	License Requirement
ASA 5580, ASA 5585-X	Cluster License, supports up to 8 units. A Cluster license is required on each unit. For other feature licenses, cluster units do not require the same license on each unit. If you have feature licenses on multiple units, they combine into a single running ASA cluster license. **Note** Each unit must have the same encryption license and the same 10 GE I/O license.
ASA 5512-X[1]	Security Plus license, supports 2 units. **Note** Each unit must have the same encryption license.
ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X[1]	Base License, supports 2 units. **Note** Each unit must have the same encryption license.
All other models	No support.

[1] Supported in 9.1(4) and later.

Prerequisites for ASA Clustering

Switch Prerequisites

- Be sure to complete the switch configuration before you configure clustering on the ASAs.
- Table 8-2 lists supported external hardware and software to interoperate with ASA clustering.

Table 8-2 External Hardware and Software Dependencies for ASA Clustering

External Hardware	External Software	ASA Version
Nexus 7000	NXOS 5.2(5) and later	9.0(1) and later.
Nexus 5000	NXOS 7.0(1) and later	9.1(4) and later.
Catalyst 6500 with Supervisor 32, 720, and 720-10GE	IOS 12.2(33)SXI7, SXI8, and SXI9 and later	9.0(1) and later.
Catalyst 3750-X	IOS 15.0(2) and later	9.1(4) and later.

ASA Prerequisites

- Provide each unit with a unique IP address before you join them to the management network.

  - See Chapter 3, “Getting Started,” 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. See the “Enabling Jumbo Frame Support (Supported Models)” section on page 9-35.
- See also the “ASA Hardware and Software Requirements” section on page 8-3.

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.

Guidelines and Limitations

Context Mode Guidelines

Supported in single and multiple context modes. The mode must match on each member unit.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes. For single mode, the firewall mode must match on all units.

Failover Guidelines

Failover is not supported with clustering.

IPv6 Guidelines

Supports IPv6. However, the cluster control link is only supported using IPv4.

Model Guidelines

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. See the “Sizing the Cluster Control Link” section on page 8-7 for more information.
- ASA 5580
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X

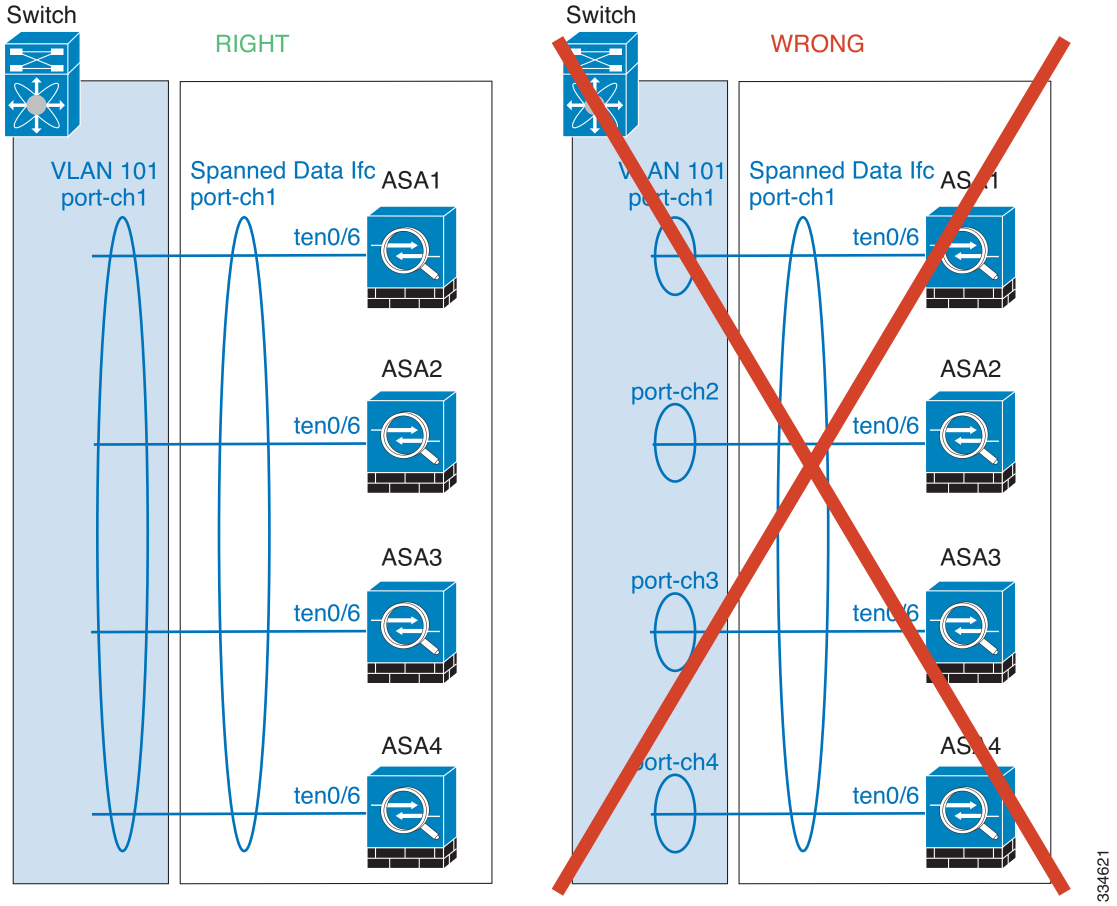
Switch Guidelines

- 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.

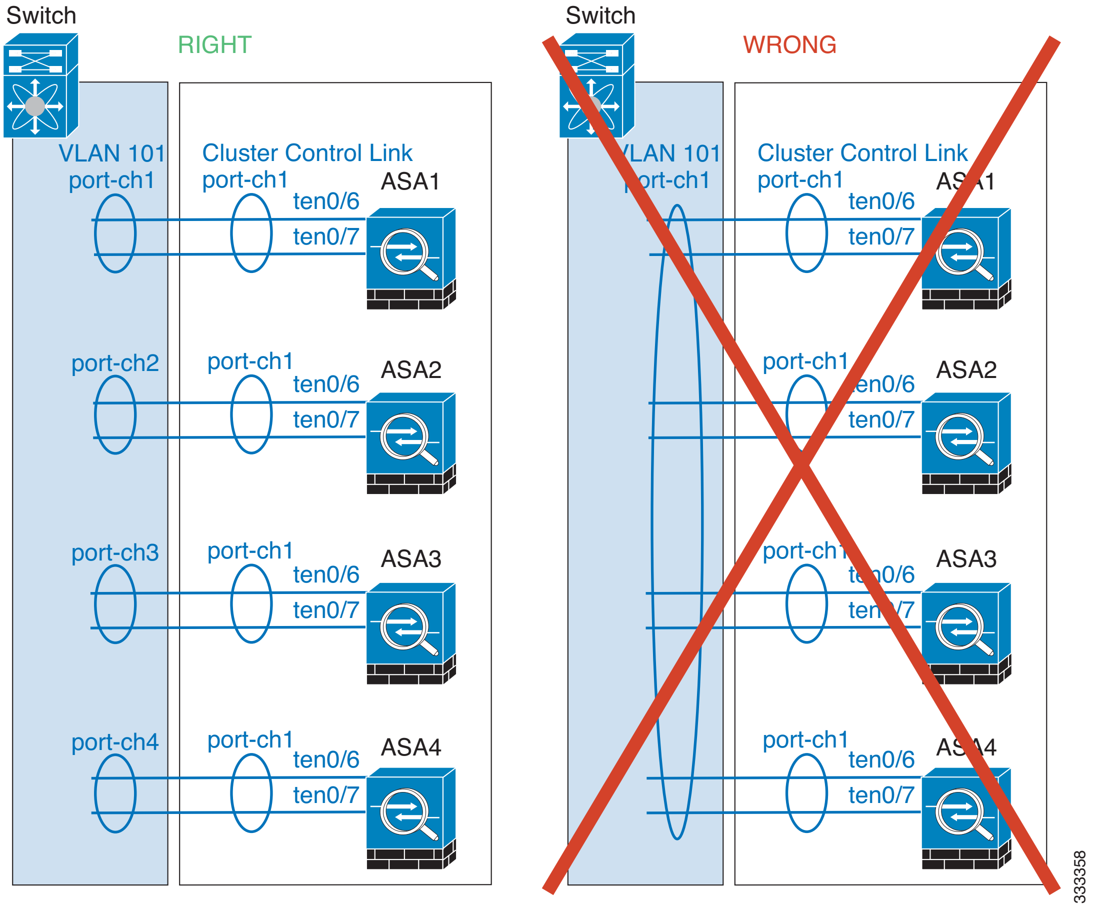
- When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an Individual interface on the switch.
- On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: **source-dest-ip** or **source-dest-ip-port** (see the Nexus OS and 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 Nexus switches.

EtherChannel Guidelines

- 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.
- For detailed EtherChannel guidelines, limitations, and prerequisites, see the "Configuring an EtherChannel" section on page 9-30.
- See also the "EtherChannel Guidelines" section on page 9-13.
- 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

- See the "ASA Hardware and Software Requirements" section on page 8-3.
- For unsupported features with clustering, see the "Unsupported Features" section on page 8-20.
- 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.

Default Settings

- 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.

Configuring ASA Clustering

Note To enable or disable clustering, you must use a console connection (for CLI) or an ASDM connection.

- Task Flow for ASA Cluster Configuration, page 8-32
- Cabling the Cluster Units and Configuring Upstream and Downstream Equipment, page 8-33
- Configuring the Cluster Interface Mode on Each Unit, page 8-35
- Configuring Interfaces on the Master Unit, page 8-36
- Configuring the Master Unit Bootstrap Settings, page 8-42
- Configuring Slave Unit Bootstrap Settings, page 8-48

Task Flow for ASA Cluster Configuration

To configure clustering, perform the following steps:

Step 1 Complete all pre-configuration on the switches and ASAs according to the "Prerequisites for ASA Clustering" section on page 8-27.

Step 2 Cable your equipment. Before configuring clustering, cable the cluster control link network, management network, and data networks. See the "Cabling the Cluster Units and Configuring Upstream and Downstream Equipment" section on page 8-33.

Step 3 Configure the interface mode. You can only configure one type of interface for clustering: Spanned EtherChannels or Individual interfaces. See the "Configuring the Cluster Interface Mode on Each Unit" section on page 8-35.

Step 4 Configure interfaces for clustering on the master unit. You cannot enable clustering if the interfaces are not cluster-ready. See the "Configuring Interfaces on the Master Unit" section on page 8-36.

Step 5 Configure the bootstrap settings and enable clustering on the master unit. See the "Configuring the Master Unit Bootstrap Settings" section on page 8-42.

Step 6 Configure the bootstrap settings for each slave unit. See the "Configuring Slave Unit Bootstrap Settings" section on page 8-48.

Step 7 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. For a list of supported and unsupported features, see the "ASA Features and Clustering" section on page 8-20.

Cabling the Cluster Units and Configuring 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.

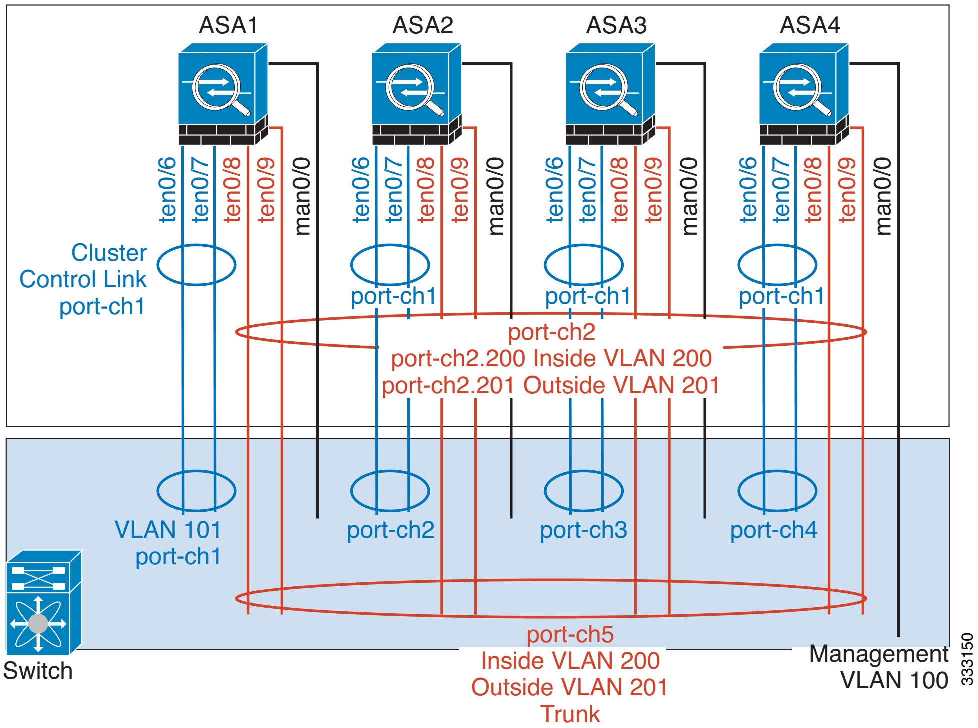
Examples

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.



Purpose	Connect Interfaces on each of 4 ASAs	To Switch Ports
Cluster control link	TenGigabitEthernet 0/6 and TenGigabitEthernet 0/7	8 ports total 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.
Inside and outside interfaces	TenGigabitEthernet 0/8 and TenGigabitEthernet 0/9	8 ports total 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.
Management interface	Management 0/0	4 ports total Place all interfaces on the same isolated management VLAN, for example VLAN 100.

What to Do Next

Configure the cluster interface mode on each unit. See the "Configuring the Cluster Interface Mode on Each Unit" section on page 8-35.

Configuring 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. For exceptions for the management interface and other guidelines, see the "Interface Type Mode" section on page 8-6.

Prerequisites

- You must set the mode separately on each ASA that you want to add to the cluster.
- Transparent firewall mode supports only Spanned EtherChannel mode.
- For multiple context mode, configure this setting in the system execution space; you cannot configure the mode per context.

Detailed Steps

	Command	Purpose
Step 1	**cluster interface-mode** {**individual** | **spanned**} **check-details** **Example:** `ciscoasa(config)# cluster interface-mode spanned check-details`	The **check-details** command shows any incompatible configuration so you can force the interface mode and fix your configuration later; the mode is not changed with this command.
Step 2	**cluster interface-mode** {**individual** | **spanned**} **force** **Example:** `ciscoasa(config)# cluster interface-mode spanned force`	Sets the interface mode for clustering. 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 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.

What to Do Next

Configure interfaces. See the "Configuring Interfaces on the Master Unit" section on page 8-36.

Configuring 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. For more information, see the "ASA Cluster Interfaces" section on page 8-4.

- Configuring Individual Interfaces (Recommended for the Management Interface), page 8-36
- Configuring Spanned EtherChannels, page 8-38

Configuring 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. See the "Management Interface" section on page 8-11 for more information.

Prerequisites

- Except for the management-only interface, you must be in Individual interface mode; see the "Configuring the Cluster Interface Mode on Each Unit" section on page 8-35.
- For multiple context mode, perform this procedure in each context. If you are not already in the context configuration mode, enter the **changeto context** *name* command.
- Individual interfaces require you to configure load balancing on neighbor devices. External load balancing is not required for the management interface. For information about load balancing, see the "Load Balancing Methods" section on page 8-13.
- (Optional) Configure the interface as a device-local EtherChannel interface, a redundant interface, and/or configure subinterfaces.
  - For an EtherChannel, see the "Configuring an EtherChannel" section on page 9-30. This EtherChannel is local to the unit, and is not a Spanned EtherChannel.
  - For a redundant interface, see the "Configuring a Redundant Interface" section on page 9-28. Management-only interfaces cannot be redundant interfaces.
  - For subinterfaces, see the "Configuring VLAN Subinterfaces and 802.1Q Trunking" section on page 9-33.

Detailed Steps

	Command	Purpose

Step 1	(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`
		Configures a pool of Local IP addresses (IPv4 and/or IPv6), one of which will be assigned to each cluster unit for the interface. 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	**interface** *interface_id* **Example:** `ciscoasa(config)# interface tengigabitethernet 0/8`	Enters interface configuration mode.
Step 3	(Management interface only) **management-only** **Example:** `ciscoasa(config-if)# management-only`	Sets an interface to management-only mode so that it does not pass through traffic. 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	**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.

Step 5	(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`
		Sets the Main cluster IP address and identifies the cluster pool. 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.

	Command	Purpose
Step 6	**security-level** *number* **Example:** `ciscoasa(config-if)# security-level 100`	Sets the security level, where *number* is an integer between 0 (lowest) and 100 (highest). See the "Security Levels" section on page 11-1.
Step 7	**no shutdown** **Example:** `ciscoasa(config-if)# no shutdown`	Enables the interface.

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
```

What to Do Next

- For spanned interface mode, configure your data interfaces. See the "Configuring Spanned EtherChannels" section on page 8-38.
- For Individual interface mode, join the cluster. See the "Configuring the Master Unit Bootstrap Settings" section on page 8-42.

Configuring Spanned EtherChannels

A Spanned EtherChannel spans all ASAs in the cluster, and provides load balancing as part of the EtherChannel operation.

Prerequisites

- You must be in Spanned EtherChannel interface mode; see the "Configuring the Cluster Interface Mode on Each Unit" section on page 8-35.
- 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 according to the "Configuring Bridge Groups" section on page 12-8.

Guidelines

- *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 Nexus OS and 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 (see the "Configuring the Master Unit Bootstrap Settings" section on page 8-42). This requirement prevents traffic from being forwarded to a unit that is not an active unit in the cluster.
- For detailed EtherChannel guidelines, limitations, and prerequisites, see the "Configuring an EtherChannel" section on page 9-30.
- See also the "EtherChannel Guidelines" section on page 9-13.

Detailed Steps

	Command	Purpose
Step 1	**interface** *physical_interface* **Example:** `ciscoasa(config)# interface gigabitethernet 0/0`	Specifies the interface you want to add to the channel group, where 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	**channel-group** *channel_id* **mode active** [**vss-id** {**1** | **2**}] **Example:** `ciscoasa(config-if)# channel-group 1 mode active`	Assigns this interface to an EtherChannel with the *channel_id* 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. See also the "Connecting to a VSS or vPC" section on page 8-14 for more information.
Step 3	**no shutdown** **Example:** `ciscoasa(config-if)# no shutdown`	Enables the interface.

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 an EtherChannel, can have only 8 active interfaces out of 16 maximum; the remaining 8 interfaces are on standby in case of link failure. For example, for a cluster of 8 ASAs, you can use a maximum of 2 interfaces on each ASA, for a total of 16 interfaces in the EtherChannel.

Step 5	**interface port-channel** *channel_id* **Example:** `ciscoasa(config)# interface port-channel 1`	Specifies the port-channel interface. This interface was created automatically when you added an interface to the channel group.
Step 6	**port-channel span-cluster** [**vss-load-balance**] **Example:** `ciscoasa(config-if)# port-channel span-cluster`	Sets this EtherChannel as a Spanned EtherChannel. 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).

	Command	Purpose
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. See the "Enabling the Physical Interface and Configuring Ethernet Parameters" section on page 9-26 for Ethernet commands.

Step 8	(Optional)
	If you are creating VLAN subinterfaces on this EtherChannel, do so now. The rest of this procedure applies to the subinterfaces.
	Example:
	`ciscoasa(config)# interface port-channel 1.10`
	`ciscoasa(config-if)# vlan 10`
		See the "Configuring VLAN Subinterfaces and 802.1Q Trunking" section on page 9-33.

Step 9	(Multiple Context Mode)
	Allocate the interface to a context. See the "Configuring a Security Context" section on page 6-19.
	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	**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.
Step 11	Perform one of the following, depending on the firewall mode:	

	Routed Mode:
	(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`
	`ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32`
		Sets the IPv4 and/or IPv6 address. DHCP, PPPoE, and IPv6 autoconfig are not supported.

	Command	Purpose
	Transparent Mode: **bridge-group** *number* **Example:** `ciscoasa(config-if)# bridge-group 1`	Assigns the interface to a bridge group, 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	**security-level** *number* **Example:** `ciscoasa(config-if)# security-level 50`	Sets the security level, where *number* is an integer between 0 (lowest) and 100 (highest). See the "Security Levels" section on page 11-1.
Step 13	**mac-address** *mac_address* **Example:** `ciscoasa(config-if)# mac-address 000C.F142.4CDE`	You must configure a MAC address for a Spanned EtherChannel so that the MAC address does not change when the current master unit leaves the cluster; 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 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.

What to Do Next

Configure the master unit bootstrap settings. See the "Configuring the Master Unit Bootstrap Settings" section on page 8-42.

Configuring 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.

- Prerequisites, page 8-42
- Enabling the Cluster Control Link Interface, page 8-43
- Configuring Basic Bootstrap Settings and Enabling Clustering, page 8-45
- Configuring Advanced Clustering Settings, page 8-47
- Examples, page 8-48

Prerequisites

- 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 **changeto system** command.
- We recommend enabling jumbo frame reservation for use with the cluster control link. See the "Enabling Jumbo Frame Support (Supported Models)" section on page 9-35.
- 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 according to the "Configuring Interfaces on the Master Unit" section on page 8-36 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.

Enabling the Cluster Control Link Interface

You need to 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.

Prerequisites

Determine the size of the cluster control link by referring to the "Sizing the Cluster Control Link" section on page 8-7.

Restrictions

- 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.

Detailed Steps—Single Interface

	Command	Purpose

Step 1	**`interface`** *`interface_id`*
	Example:
	`ciscoasa(config)# interface tengigabitethernet 0/6`
		Enters interface configuration mode.

Step 2	**`no shutdown`**
	Example:
	`ciscoasa(config-if)# no shutdown`
		Enables the interface. You only need to enable the interface; do not configure a name for the interface, or any other parameters.

Detailed Steps—EtherChannel Interface

	Command	Purpose

Step 1	**`interface`** *`interface_id`*
	Example:
	`ciscoasa(config)# interface tengigabitethernet 0/6`
		Enters interface configuration mode.

Step 2	**`channel-group`** *`channel_id`* **`mode on`**
	Example:
	`ciscoasa(config-if)# channel-group 1 mode on`
		Assigns this physical interface to an EtherChannel with the *channel_id* 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*
		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.

Step 3	**`no shutdown`**
	Example:
	`ciscoasa(config-if)# no shutdown`
		Enables the interface.

Step 4	**`interface`** *`interface_id`*
	  `channel-group` *`channel_id`* **`mode on`**
	  `no shutdown`
	Example:
	`ciscoasa(config)# interface tengigabitethernet 0/7`
	`ciscoasa(config-if)# channel-group 1 mode on`
	`ciscoasa(config-if)# no shutdown`
		Repeat for each additional interface you want to add to the EtherChannel.

What to Do Next

Configure the master unit bootstrap settings. See the Configuring Basic Bootstrap Settings and Enabling Clustering, page 8-45.

Configuring Basic Bootstrap Settings and Enabling Clustering

Perform the following steps to configure basic bootstrap settings and to enable clustering.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **mtu cluster** *bytes* **Example:** `ciscoasa(config)# mtu cluster 9000`	Specifies the maximum transmission unit for the cluster control link interface, between 64 and 65,535 bytes. The default MTU is 1500 bytes. **Note** We suggest setting the MTU to 1600 bytes or greater, which requires you to enable jumbo frame reservation before continuing with this procedure. See the "Enabling Jumbo Frame Support (Supported Models)" section on page 9-35. 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 2	**cluster group** *name* **Example:** `ciscoasa(config)# cluster group pod1`	Names the cluster and enters cluster configuration mode. 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 3	**local-unit** *unit_name* **Example:** `ciscoasa(cfg-cluster)# local-unit unit1`	Names this member of the cluster with 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 4	**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`
		Specifies the cluster control link interface, preferably an EtherChannel. Subinterfaces and Management interfaces are not allowed. See the "Configuring Interfaces on the Master Unit" section on page 8-36
		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 5	**priority** *priority_number* **Example:** `ciscoasa(cfg-cluster)# priority 1`	Sets the priority of this unit for master unit elections, between 1 and 100, where 1 is the highest priority. See the "Master Unit Election" section on page 8-3 for more information.

<table>
<tr><th></th><th>Command</th><th>Purpose</th></tr>
<tr><td><b>Step 6</b></td><td>(Optional)
<b>key</b> <i>shared_secret</i>
<b>Example:</b><pre>ciscoasa(cfg-cluster)# key
chuntheunavoidable</pre></td><td>Sets an authentication key for control traffic on the cluster control link. 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.</td></tr>
<tr><td><b>Step 7</b></td><td>(Optional)
<b>clacp system-mac</b> {<i>mac_address</i> | <b>auto</b>} [<b>system-priority</b> <i>number</i>]
<b>Example:</b><pre>ciscoasa(cfg-cluster)# clacp system-mac
000a.0000.aaaa</pre></td><td>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 <i>H.H.H</i>, 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 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.</td></tr>
<tr><td><b>Step 8</b></td><td><b>enable</b> [<b>noconfirm</b>]
<b>Example:</b><pre>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</pre></td><td>Enables clustering. When you enter the <b>enable</b> 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 <b>No</b>, then clustering is not enabled. Use the <b>noconfirm</b> 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 <b>no enable</b> command.

<b>Note</b> If you disable clustering, all data interfaces are shut down, and only the management-only interface is active. If you want to remove the unit from the cluster entirely (and thus want to have active data interfaces), see the “Leaving the Cluster” section on page 8-56.</td></tr>
</table>

What to Do Next

- Configure advanced settings. See the “Configuring Advanced Clustering Settings” section on page 8-47.
- Add slave units. See the “Configuring Slave Unit Bootstrap Settings” section on page 8-48.

Configuring Advanced Clustering Settings

Perform the following steps to customize your clustering configuration.

Detailed Steps

	Command	Purpose
Step 1	**health-check** [**holdtime** *timeout*] **Example:** `ciscoasa(cfg-cluster)# health-check holdtime 5`	Customizes the cluster health check feature, which includes unit health monitoring and interface health monitoring. The **holdime** 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. The interface health check monitors for link failures. If an interface fails on a particular unit, but the same interface is active 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 details, see Interface monitoring, page 8-9. Health check is enabled by default. You can disable it using the **no** form of this command. **Note** 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 2	**conn-rebalance** [**frequency** *seconds*] **Example:** `ciscoasa(cfg-cluster)# conn-rebalance frequency 60`	Enables connection rebalancing for TCP traffic. 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. **Note**

	Command	Purpose
Step 3	**console-replicate** **Example:** ciscoasa(cfg-cluster)# console-replicate	Enables console replication from slave units to the master unit. 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 you only need to monitor one console port for the cluster.

What to Do Next

Add slave units. See the "Configuring Slave Unit Bootstrap Settings" section on page 8-48.

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
    no shutdown

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 unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

Configuring Slave Unit Bootstrap Settings

Perform the following procedures to configure the slave units.

- Prerequisites, page 8-49
- Enabling the Cluster Control Link Interface, page 8-49
- Configuring Bootstrap Settings and Joining the Cluster, page 8-50
- Examples, page 8-52

Prerequisites

- 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. See the "Enabling Jumbo Frame Support (Supported Models)" section on page 9-35.
- 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.

Enabling the Cluster Control Link Interface

Configure the same cluster control link interface as you configured for the master unit. See the "Enabling the Cluster Control Link Interface" section on page 8-43.

Detailed Steps—Single Interface

	Command	Purpose

Step 1	**`interface`** *`interface_id`*
	Example:
	`ciscoasa(config)# interface tengigabitethernet 0/6`
		Enters interface configuration mode.

Step 2	**`no shutdown`**
	Example:
	`ciscoasa(config-if)# no shutdown`
		Enables the interface. You only need to enable the interface; do not configure a name for the interface, or any other parameters.

Detailed Steps—EtherChannel Interface

	Command	Purpose

Step 1	**`interface`** *`interface_id`*
	Example:
	`ciscoasa(config)# interface tengigabitethernet 0/6`
		Enters interface configuration mode.

Step 2	**`channel-group`** *`channel_id`* **`mode on`**
	Example:
	`ciscoasa(config-if)# channel-group 1 mode on`
		Assigns this physical interface to an EtherChannel with the *channel_id* 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*
		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.

Step 3	**`no shutdown`**
	Example:
	`ciscoasa(config-if)# no shutdown`
		Enables the interface.

Step 4	**`interface`** *`interface_id`*
	`  channel-group` *`channel_id`* **`mode on`**
	`  no shutdown`
	Example:
	`ciscoasa(config)# interface tengigabitethernet 0/7`
	`ciscoasa(config-if)# channel-group 1 mode on`
	`ciscoasa(config-if)# no shutdown`
		Repeat for each additional interface you want to add to the EtherChannel.

What to Do Next

Configure the slave unit bootstrap settings. See the Configuring Bootstrap Settings and Joining the Cluster, page 8-50.

Configuring Bootstrap Settings and Joining the Cluster

Perform the following steps to configure bootstrap settings and join the cluster as a slave unit.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **mtu cluster** *bytes* **Example:** `ciscoasa(config)# mtu cluster 9000`	Specifies the same MTU that you configured for the master unit. **Note** We suggest setting the MTU to 1600 bytes or greater, which requires you to enable jumbo frame reservation before continuing with this procedure. See the "Enabling Jumbo Frame Support (Supported Models)" section on page 9-35. Jumbo frame reservation requires a reload of the ASA.
Step 2	**cluster group** *name* **Example:** `ciscoasa(config)# cluster group pod1`	Identifies the same cluster name that you configured for the master unit.
Step 3	**local-unit** *unit_name* **Example:** `ciscoasa(cfg-cluster)# local-unit unit1`	Names this member of the cluster with 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 4	**cluster-interface** *interface_id* **ip** *ip_address mask*
	Example:
	`ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0`
	`INFO: Non-cluster interface config is cleared on Port-Channel2`
		Specifies the same cluster control link interface that you configured for the master unit.
		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 5	**priority** *priority_number* **Example:** `ciscoasa(cfg-cluster)# priority 2`	Sets the priority of this unit for master unit elections, between 1 and 100, where 1 is the highest priority. See the "Master Unit Election" section on page 8-3 for more information.

	Command	Purpose
Step 6	(Optional) **key** *shared_secret* **Example:** `ciscoasa(cfg-cluster)# key chuntheunavoidable`	Sets the same authentication key that you set for the master unit.
Step 7	**enable as-slave** **Example:** `ciscoasa(cfg-cluster)# enable as-slave`	Enables clustering. 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. If you want to remove the unit from the cluster entirely (and thus want to have active data interfaces), see the "Leaving the Cluster" section on page 8-56.

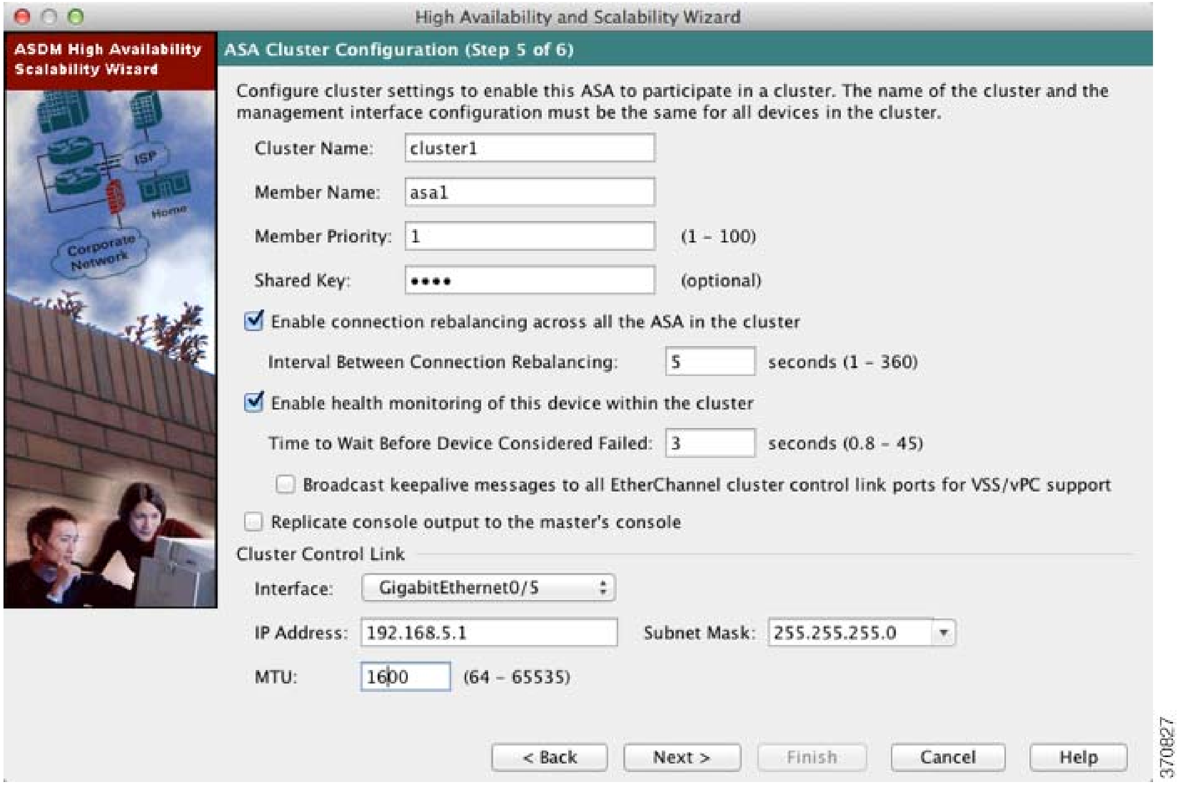
What to Do Next

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. For a list of supported and unsupported features, see the "ASA Features and Clustering" section on page 8-20.

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
```



High Availability and Scalability Wizard
ASDM High Availability Scalability Wizard
ISP
Home
Corporate Network
< Back
Next >
Finish
Cancel
Help
370827

ASA Cluster Configuration (Step 5 of 6)

Configure cluster settings to enable this ASA to participate in a cluster. The name of the cluster and the management interface configuration must be the same for all devices in the cluster.

Cluster Name: cluster1

Member Name: asa1

Member Priority: 1 (1 - 100)

Shared Key: •••• (optional)

☑ Enable connection rebalancing across all the ASA in the cluster

Interval Between Connection Rebalancing: 5 seconds (1 - 360)

☑ Enable health monitoring of this device within the cluster

Time to Wait Before Device Considered Failed: 3 seconds (0.8 - 45)

□ Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support

□ Replicate console output to the master's console

Cluster Control Link

Interface: GigabitEthernet0/5

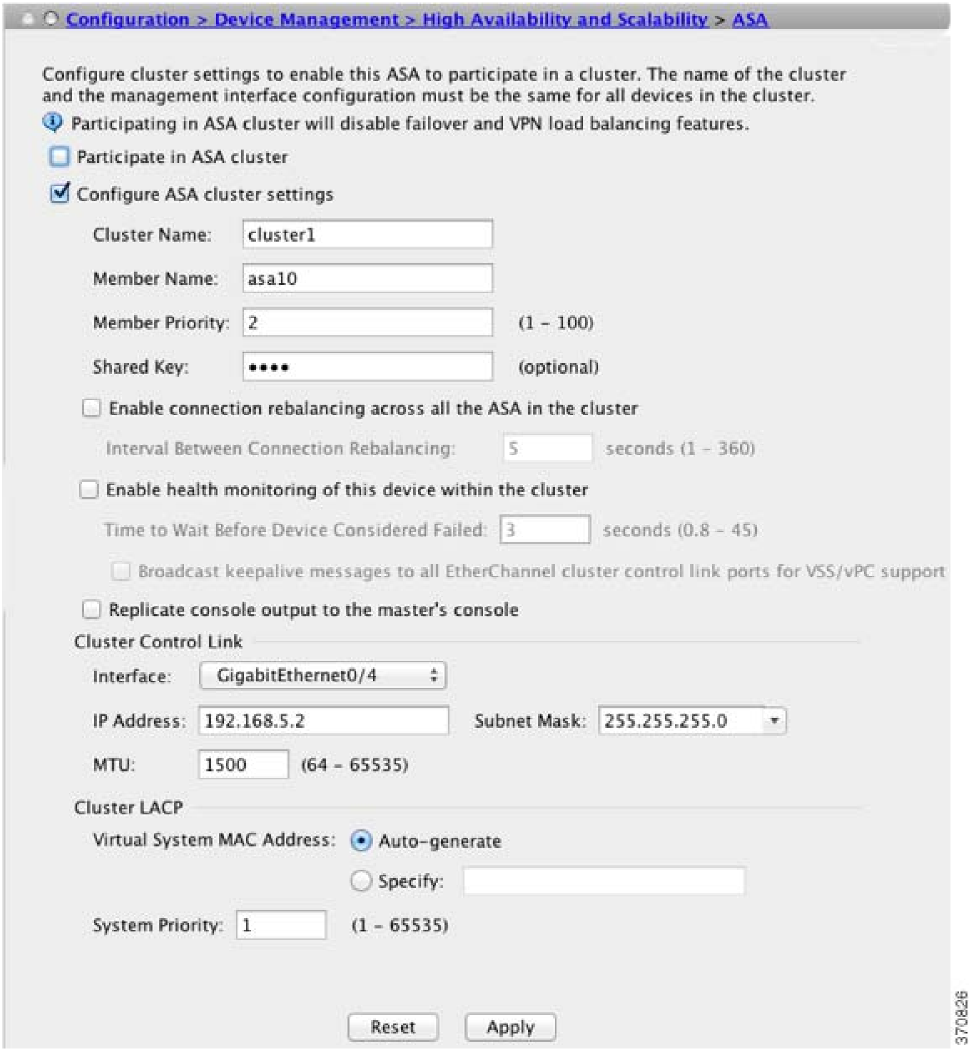
IP Address: 192.168.5.1 Subnet Mask: 255.255.255.0

MTU: 1600 (64 - 65535)

Note Do not configure connection rebalancing for inter-site topologies; you do not want connections rebalanced to cluster members at a different site.

– (Optional) **Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support**—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 this 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 this option, 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.

Managing ASA Cluster Members



Configuration > Device Management > High Availability and Scalability > ASA

Configure cluster settings to enable this ASA to participate in a cluster. The name of the cluster and the management interface configuration must be the same for all devices in the cluster.

Participating in ASA cluster will disable failover and VPN load balancing features.

□ Participate in ASA cluster

☑ Configure ASA cluster settings

Cluster Name: cluster1

Member Name: asa10

Member Priority: 2 (1 - 100)

Shared Key: •••• (optional)

□ Enable connection rebalancing across all the ASA in the cluster

Interval Between Connection Rebalancing: 5 seconds (1 - 360)

□ Enable health monitoring of this device within the cluster

Time to Wait Before Device Considered Failed: 3 seconds (0.8 - 45)

□ Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support

□ Replicate console output to the master's console

Cluster Control Link

Interface: GigabitEthernet0/4

IP Address: 192.168.5.2 Subnet Mask: 255.255.255.0

MTU: 1500 (64 - 65535)

Cluster LACP

Virtual System MAC Address: ● Auto-generate

○ Specify:

System Priority: 1 (1 - 65535)

– (Optional) Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support—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 this 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 this option, 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.

Becoming an Inactive Member

To become an inactive member of the cluster, disable clustering on the unit while leaving the clustering configuration intact.

Note 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. See the "Leaving the Cluster" section on page 8-56. 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.

Prerequisites

- 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 **changeto system** command.

Detailed Steps

	Command	Purpose
Step 1	**cluster group** *name* **Example:** `ciscoasa(config)# cluster group pod1`	Enters cluster configuration mode.
Step 2	**no enable** **Example:** `ciscoasa(cfg-cluster)# no enable`	Disables clustering. 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 you can enable clustering again later.

Inactivating a Member

To inactivate a member from any unit, perform the following steps.

Note 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. See the "Leaving the Cluster" section on page 8-56. 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.

Prerequisites

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.

Detailed Steps

Command	Purpose

`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`
	Removes the unit from the cluster. The bootstrap configuration remains intact, as well as the last configuration synced from the master unit, so 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.

Leaving 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.

Prerequisites

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.

Detailed Steps

	Command	Purpose

Step 1	For a slave unit:
	`cluster group` *`cluster_name`*
	    `no enable`
	Example:
	`ciscoasa(config)# cluster group cluster1`
	`ciscoasa(cfg-cluster)# no enable`
		Disables clustering. You cannot make configuration changes while clustering is enabled on a slave unit.

Step 2	**`clear configure cluster`**
	Example:
	`ciscoasa(config)# clear configure cluster`
		Clears the cluster configuration. The ASA shuts down all interfaces including the management interface and cluster control link.

	Command	Purpose

Step 3	**`no cluster interface-mode`**
	Example:
	`ciscoasa(config)# no cluster interface-mode`
		Disables 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` *`backup_cfg`* **`running-config`**
	Example:
	`ciscoasa(config)# copy backup_cluster.cfg running-config`
	`Source filename [backup_cluster.cfg]?`
	`Destination filename [running-config]?`
	`ciscoasa(config)#`
		Copies the backup configuration to the running configuration.

Step 5	**`write memory`**
	Example:
	`ciscoasa(config)# write memory`
		Saves the configuration to startup.

Step 6	If you do not have a backup configuration, reconfigure management access according to Chapter 3, “Getting Started.” Be sure to change the interface IP addresses, and restore the correct hostname, for example.	

Changing the Master Unit

Caution The best method to change the master unit is to disable clustering on the master unit (see the “Becoming an Inactive Member” section on page 8-54), 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. See the “Centralized Features” section on page 8-21 for a list of centralized features.

To change the master unit, perform the following steps.

Prerequisites

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.

Detailed Steps

Command	Purpose
cluster master unit *unit_name* **Example:** `ciscoasa(config)# cluster master unit asa2`	Sets a new unit as the master unit. 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.

Executing 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.

Detailed Steps

Command	Purpose
cluster exec [**unit** *unit_name*] *command* **Example:** `ciscoasa# cluster exec show xlate`	Sends a command to all members, or if you specify the unit name, a specific member. 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)
 secondary:*****************************************************************
 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

Monitoring Commands

To monitor the cluster, enter one of the following commands:

Command	Purpose
show cluster info [**conn-distribution** | **packet-distribution** | **health** | **loadbalance** | **trace**]	With no keywords, the **show cluster info** command shows the status of all members of the cluster. 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 trace** command shows the debug information for further troubleshooting. The **show cluster info health** command shows the current health of interfaces, units, and the cluster overall. The **show cluster info loadbalance** command shows connection rebalance statistics.
show cluster {**access-list** | **conn** | **cpu** | **history** | **interface-mode** | **memory** | **resource** | **traffic** | **xlate**} [*options*]	Displays aggregated data for the entire cluster. The *options* available depends on the data type.
show cluster user-identity [*options*]	Displays cluster-wide user identity information and statistics.
show lacp cluster {**system-mac** | **system-id**}	Shows the cLACP system ID and priority.
debug cluster [**ccp** | **datapath** | **fsm** | **general** | **hc** | **license** | **rpc** | **transport**]	Shows debug messages for clustering.
debug lacp cluster [**all** | **ccp** | **misc** | **protocol**]	Shows debug messages for cLACP.
show asp cluster counter	This command is useful for datapath troubleshooting.

Example 8-1 show cluster info

```
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)
      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
```

Example 8-2 show cluster info trace

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

Example 8-3 show cluster access-list

```
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) 0xfe4f4947
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) 0x1e68697c
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) 0x4143a818
```

```
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
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
```

Related Commands

Command	Purpose
show conn [**detail**]	The **show conn** command shows whether a flow is a director, backup, or forwarder flow. For details about the different roles for a connection, see the “Connection Roles” section on page 8-18. 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.
show route cluster **debug route cluster**	Shows cluster information for routing.
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. See the “Capturing Packets” section on page 43-2.
mac-address pool *name start_mac_address* **-** *end_mac_address*	Creates a MAC address pool for an individual interface.
prompt cluster-unit	Sets the CLI prompt to include the cluster unit name. See the “Customizing a CLI Prompt” section on page 41-8.

Command	Purpose
`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. See the "Including the Device ID in Non-EMBLEM Format Syslog Messages" section on page 44-18.
`show port-channel`	Includes information about whether a port-channel is spanned.

Example 8-4 show conn

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 ASA 1 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
```

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 - inbound data,
            i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
            k - Skinny media, 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,
            s - awaiting outside 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, timeout 30s, 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 -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes
1580, cluster sent/rcvd bytes 0/0, 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)
```

Configuration Examples for ASA Clustering

- Sample ASA and Switch Configuration, page 8-63
- Firewall on a Stick, page 8-66
- Traffic Segregation, page 8-68
- Redundant Interface (PBR or ECMP), page 8-70
- Spanned EtherChannel With Backup Links, page 8-72

Sample ASA and Switch Configuration

The following sample configurations connect the following interfaces between the ASA and the switch:

ASA Interface	Switch Interface
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

- ASA Configuration, page 8-63
- IOS Switch Configuration, page 8-65

ASA Configuration

Interface Mode on Each Unit

```
cluster interface-mode spanned force
```

ASA1 Master Bootstrap Configuration

```
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
 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 B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-slave
```

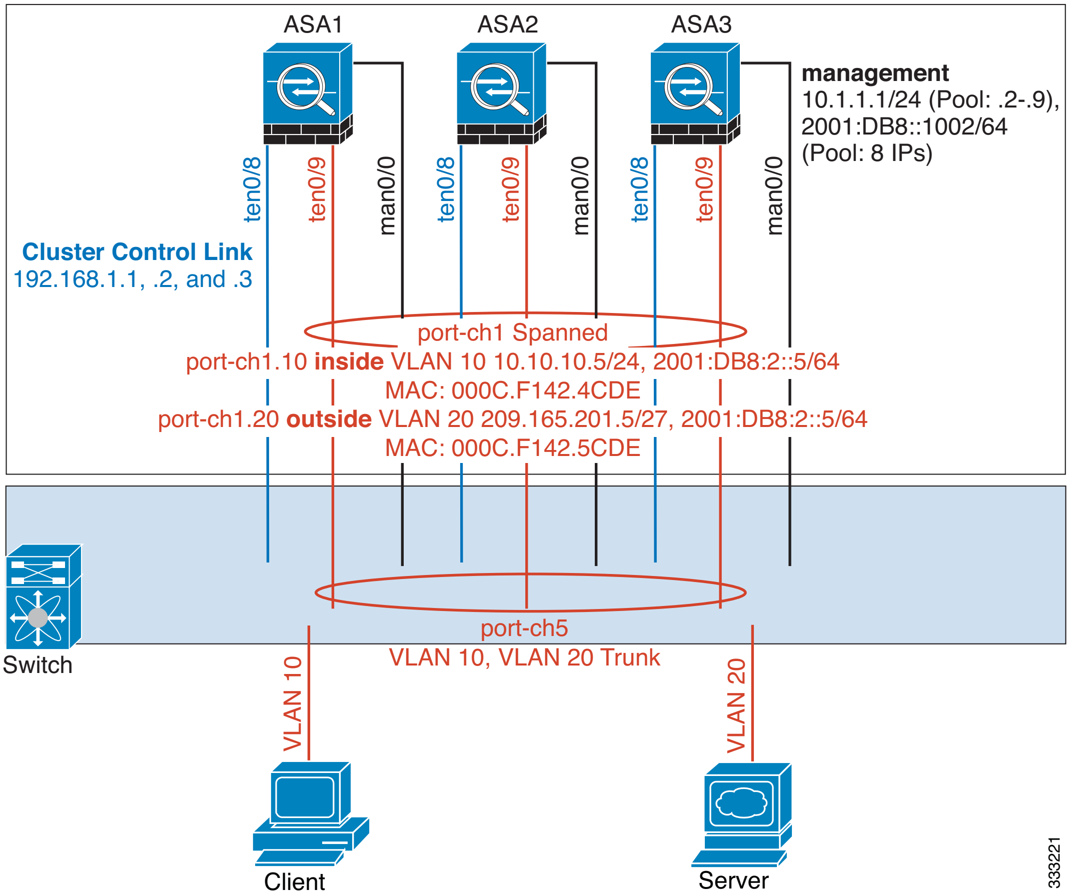
Master Interface Configuration

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 11 mode active
 no shutdown
!
interface GigabitEthernet0/5
 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
```

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
```

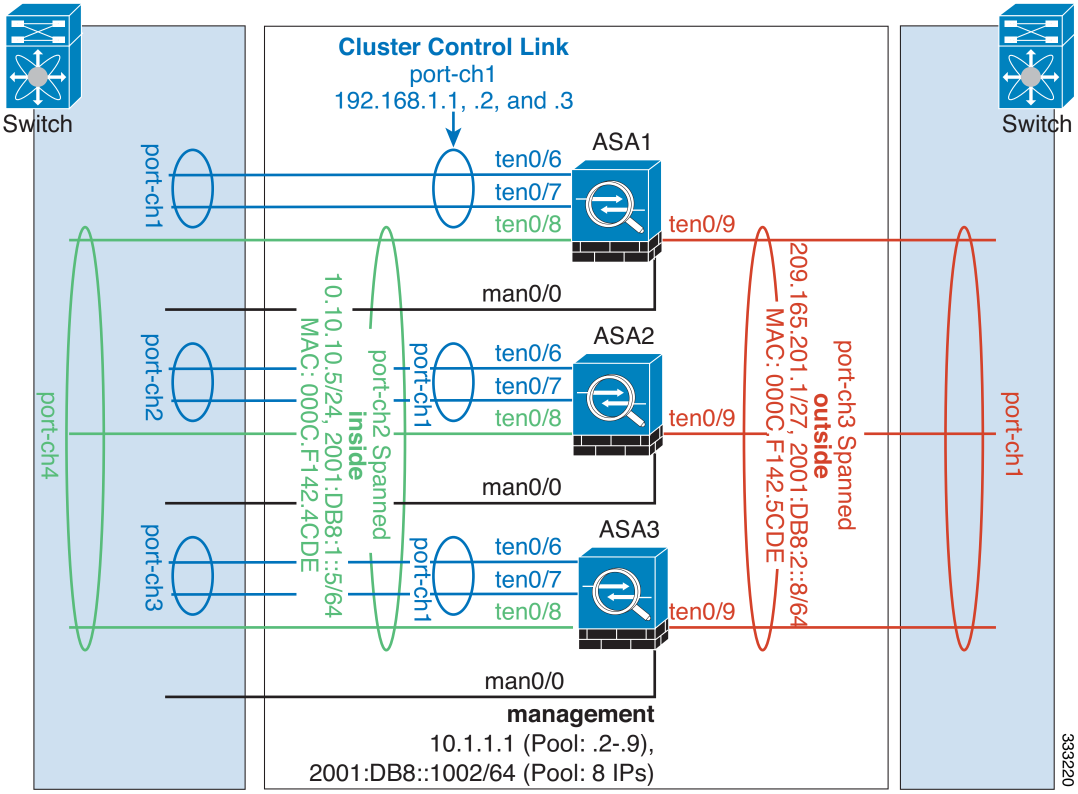
ASA3 Slave Bootstrap Configuration

```
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 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 0/9
    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

```
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 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

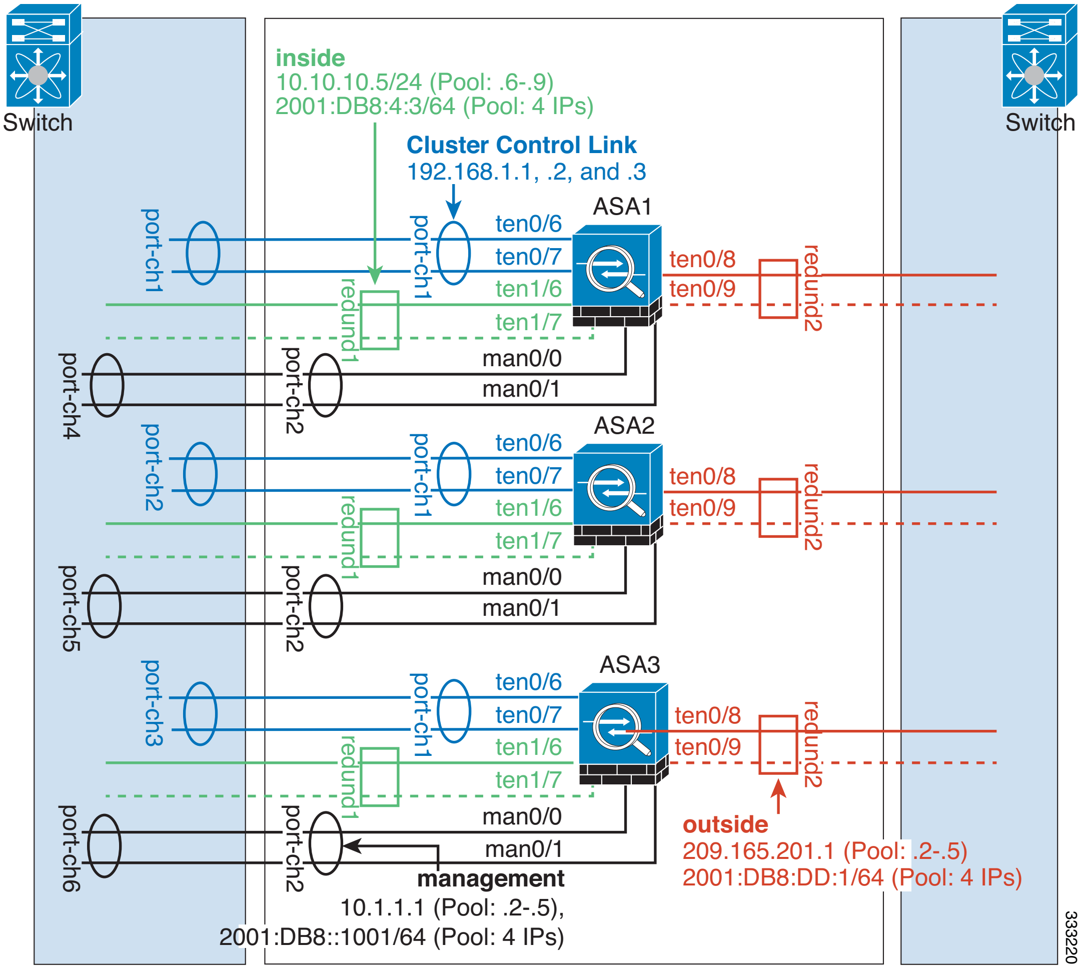
```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

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
```

```
    port-channel span-cluster
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

Redundant Interface (PBR or ECMP)



Redundant interfaces can be used to provide link-level redundancy.

When using Individual interfaces, switching to a backup interface is similar to how it behaves in non-clustering mode. The ASA activates the backup link if the primary link fails. It takes time for the Spanning Tree on the switch to converge before the backup link is activated on the switch side. The backup links can be connected to a separate switch to provide inter-switch redundancy.

Interface Mode on Each Unit

```
cluster interface-mode individual 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 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
```

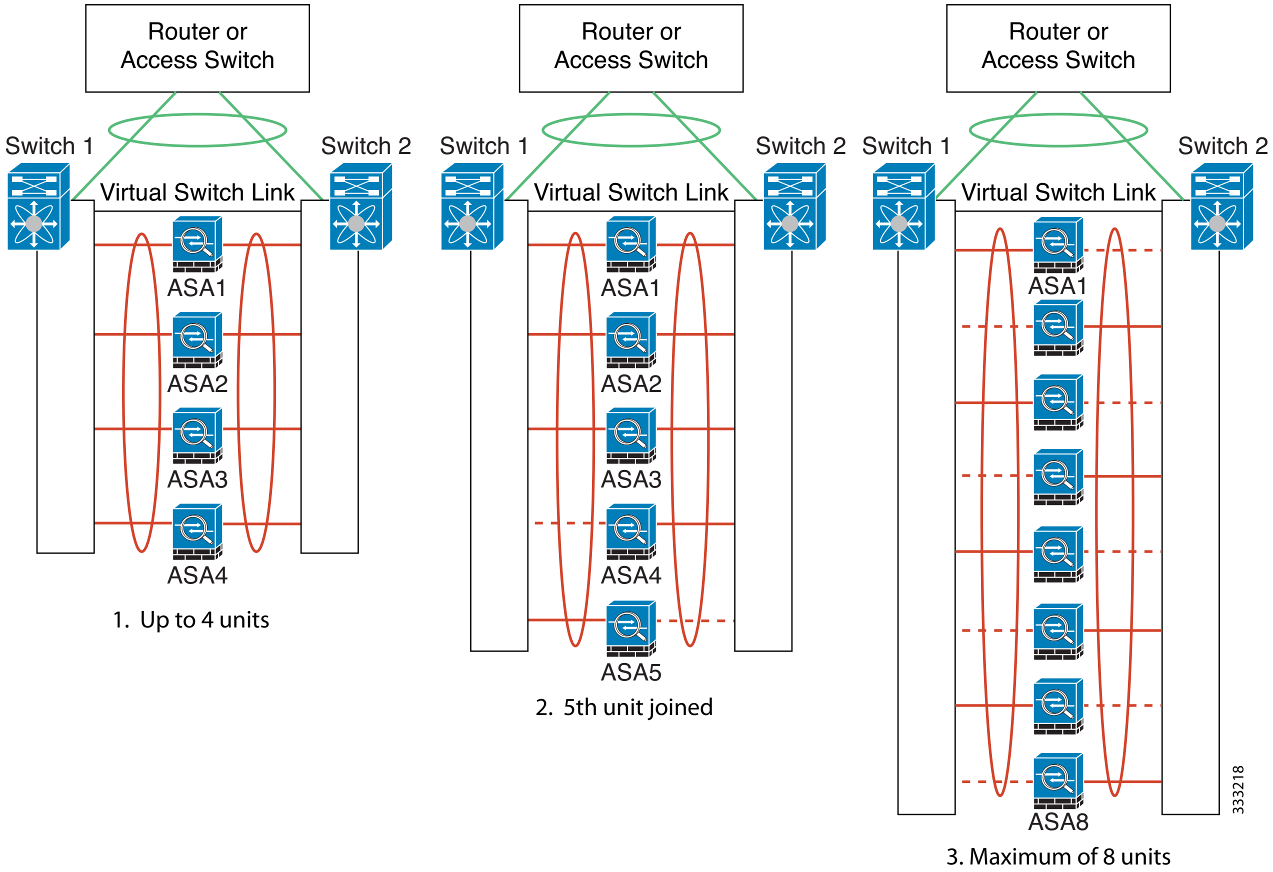
Master Interface Configuration

```
ip local pool mgmt 10.1.1.2-10.1.1.5
ipv6 local pool mgmtipv6 2001:DB8::1002/64 4

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
    ipv6 address 2001:DB8::1001/64 cluster-pool mgmtipv6
    security-level 100
    management-only

ip local pool inside 10.10.10.6-10.10.10.9
ipv6 local pool insideipv6 2001:DB8:4:4/64 4

interface redundant 1
member-interface tengigabitethernet 1/6
member-interface tengigabitethernet 1/7
    nameif inside
    ip address 10.10.10.5 255.255.255.0 cluster-pool inside
    ipv6 address 2001:DB8:4:3/64 cluster-pool insideipv6
    security-level 100

ip local pool outside 209.165.201.2-209.165.201.5
ipv6 local pool outsideipv6 2001:DB8:DD:2/64 4

interface redundant 2
member-interface tengigabitethernet 0/8
member-interface tengigabitethernet 0/9
    nameif outside
    ip address 209.165.201.1 255.255.255.224 cluster-pool outside
    ipv6 address 2001:DB8:DD:1/64 cluster-pool outsideipv6
    security-level 0
```

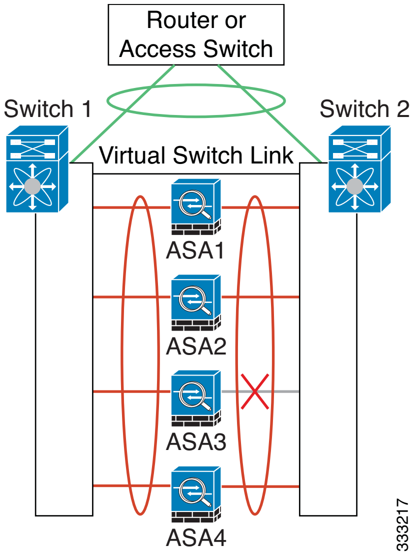
Spanned EtherChannel With Backup Links

The maximum number of active ports in an 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 VSS 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:

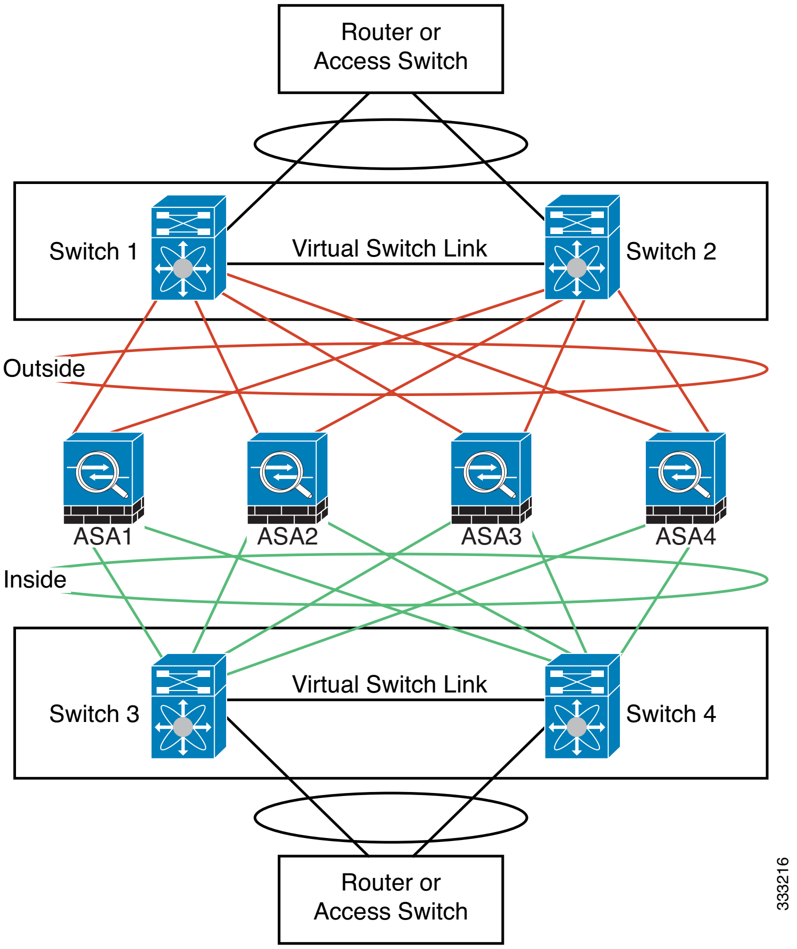


The principle is to first maximize the number of active ports in the channel, and secondly keep the number of active primary ports and the number of active secondary ports in balance. Note that when a 5th unit joins the cluster, traffic is not balanced evenly between all units.

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
```

Feature History for ASA Clustering

Table 8-3 lists each feature change and the platform release in which it was implemented.

Table 8-3 Feature History for Clustering

Feature Name	Platform Releases	Feature Information
ASA Clustering for the ASA 5580 and 5585-X	9.0(1)	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 chash-table**, **show cluster**, **show cluster info**, **show cluster user-identity**, **show lacp cluster**, **show running-config cluster**.
ASA 5500-X support for clustering	9.1(4)	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 ASDM screens.
Improved VSS and vPC support for health check monitoring	9.1(4)	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 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 screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster
Support for cluster members at different geographical locations (inter-site); Individual Interface mode only	9.1(4)	You can now place cluster members at different geographical locations when using individual interface mode. We did not modify any ASDM screens.